LogLogic McAfee ePolicy Orchestrator (ePO) Log Configuration Guide

Document Release: March 2012

Part Number: LL600048-00ELS100001

This manual supports LogLogic McAfee ePO Release 1.0 and later, and LogLogic Software Release 5.1 and later until replaced by a new edition.

© 2012 LogLogic, Inc.

Proprietary Information

This document contains proprietary and confidential information of LogLogic, Inc. and its licensors. In accordance with the license, this document may not be copied, disclosed, modified, transmitted, or translated except as permitted in writing by LogLogic, Inc.

Trademarks

LogLogic and the LogLogic logo are trademarks or registered trademarks of LogLogic, Inc. in the United States and/or foreign countries. All other company or product names are trademarks or registered trademarks of their respective owners.

Notice

The information contained in this document is subject to change at any time without notice. All warranties with respect to the software and accompanying documentation are set our exclusively in the Software License Agreement or in the Product Purchase Agreement that covers the documentation.

LogLogic, Inc.
110 Rose Orchard Way, Suite 200
San Jose, CA 95134
Tel: +1 408 215 5900
Fax: +1 408 774 1752
U.S. Toll Free: 888 347 3883
www.loglogic.com

Contents

Preface

About This Guide . . . 5
Technical Support . . . 5
Documentation Support . . . 5
Conventions . . . 6

Chapter 1 – Configuring LogLogic's McAfee ePO Log Collection

Introduction to McAfee ePO . . . 7
Prerequisites . . . 7
Configuring McAfee ePO . . . 8
    Configuring VSE Agents . . . 8
Enabling the LogLogic Appliance to Capture Log Data . . . 23
    Adding a McAfee ePO Device . . . 23
    Testing Connectivity . . . 26
Verifying the Configuration . . . 26

Chapter 2 – How LogLogic Supports McAfee ePO

How LogLogic Captures McAfee ePO Log Data . . . 28
LogLogic Real-Time Reports . . . 29
LogLogic Search Filters . . . 31

Chapter 3 – Troubleshooting

Troubleshooting . . . 35
Frequently Asked Questions . . . 36

Appendix A – Event Reference

LogLogic Support for McAfee ePO Events . . . 37

Preface

About This Guide

The LogLogic® Appliance-based solution lets you capture and manage log data from all types of log sources in your enterprise. The LogLogic support for McAfee ePolicy Orchestrator® (ePO™) enables LogLogic Appliances to capture logs from machines running McAfee ePO.

Once the logs are captured and parsed, you can generate reports and create alerts on McAfee ePO's operations. For more information on creating reports and alerts, see the *LogLogic User Guide* and *LogLogic Online Help*.

Technical Support

LogLogic is committed to the success of our customers and to ensuring our products improve customers' ability to maintain secure, reliable networks. Although LogLogic products are easy to use and maintain, occasional assistance might be necessary. LogLogic provides timely and comprehensive customer support and technical assistance from highly knowledgeable, experienced engineers who can help you maximize the performance of your LogLogic Appliances.

To reach LogLogic Customer Support:

Telephone: Toll Free, US—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Telephone: Toll Free, Canada—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Telephone: Toll Free, Mexico—1 800 957 LOGS (5647)

Toll—1 408 834 7480

Telephone: Toll Free, United Kingdom—00 800 0330 4444

Toll—01480 479391

Telephone: Toll Free, Mainland Europe—00 800 0330 4444

Toll— +44 1480 479391

Telephone: Toll Free, Japan IDC—0061 800 0330 4444

Toll— Not Available

Telephone: Toll Free, Japan KDD—0010 800 0330 4444

Toll— Not Available

Telephone: Toll Free, Brazil—0021 800 0330 4444

Toll— Not Available

Email: support@loglogic.com

You can also visit the LogLogic Support website at: http://www.loglogic.com/services/support. When contacting Customer Support, be prepared to provide:

- Your name, email address, phone number, and fax number
- Your company name and company address
- Your machine type and release version
- A description of the problem and the content of pertinent error messages (if any)

Documentation Support

Your feedback on LogLogic documentation is important to us. Send e-mail to DocComments@loglogic.com if you have questions or comments. Your comments will be reviewed and addressed by the LogLogic technical writing team.

In your e-mail message, please indicate the software name and version you are using, as well as the title and document date of your documentation.

Conventions

LogLogic documentation uses the following conventions to highlight code and command-line elements:

- A `monospace font` is used for programming elements (such as code fragments, objects, methods, parameters, and HTML tags) and system elements (such as file names, directories, paths, and URLs).
- A **`monospace bold font`** is used to distinguish system prompts or screen output from user responses, as in this example:
  `username:` **`system`**
  `home directory:` **`home\app`**
- A *`monospace italic font`* is used for placeholders, which are general names that you replace with names specific to your site, as in this example:
  `LogLogic_home_directory``\upgrade\`
- Straight brackets signal options in command-line syntax. For example:
  `ls [-AabCcdFfgiLlmnopqRrstux1] [-X attr] [path ...]`

Chapter 1 – Configuring LogLogic's McAfee ePO Log Collection

This chapter describes configuration steps involved to enable a LogLogic Appliance to capture McAfee ePO logs. The configuration steps assume that you have a functioning LogLogic Appliance that can be configured to capture McAfee ePO log data.

- Introduction to McAfee ePO 7
- Prerequisites 7
- Configuring McAfee ePO 8
- Enabling the LogLogic Appliance to Capture Log Data 23
- Verifying the Configuration 26

Introduction to McAfee ePO

McAfee VirusScan Enterprise (VSE) is a Threat Management protection solution that includes intrusion prevention and firewall support for PCs and file servers. VSE is managed using McAfee ePO, that includes security-policy compliance and reporting functionality.

The LogLogic Appliance supports McAfee VSE events that are stored on McAfee ePO servers. The LogLogic Appliance uses the LogLogic Database Collector to pull VSE logs (i.e., Event Log, Server Task Log, etc.) via JDBC connection directly from an ePO server's Microsoft SQL Server database.

The configuration procedures for McAfee ePO and the LogLogic Appliance depend upon your environment. For more information, see *How LogLogic Captures McAfee ePO Log Data* on page 28.

Prerequisites

Prior to configuring McAfee ePO and the LogLogic Appliance, ensure that you meet the following prerequisites:

- McAfee ePO version 4.0, 4.5, or 4.6 running on Microsoft Windows 2000 Service Pack 4, 2003 Service Pack 1 or later or 2008 Service Pack 2 or later.

  Note: LogLogic uses the LogLogic Database Collector to retrieve VSE log data directly from the ePO database. The LogLogic Database Collector supports the following databases for ePO version 4.0, 4.5, and 4.6:
  - Microsoft SQL Server 2008 Service Pack 1 or higher
  - Microsoft SQL Server 2005 Service Pack 1 or higher
  - Microsoft SQL Server 2005 Express
  - Microsoft SQL Server 2000 Service Pack 3a or higher
  - Microsoft SQL Server Desktop Engine (MSDE) 2000 Service Pack 3a or higher

- McAfee VSE version 8.5i or 8.7i
- Access to the ePO Admin Console with permissions to make configuration changes
- A Microsoft SQL Server User account with `db_datareader` and `public` database role access at the minimum

Note: Mixed Mode Authentication and SQL Authentication mode are required on the ePO database.

- LogLogic Appliance running Release 5.1 or later installed with a Log Source Package that includes McAfee ePO support
- Administrative access on the LogLogic Appliance

Configuring McAfee ePO

The following sections describe how to configure the ePO server as well as install and configure VSE and the ePO Agent.

Note: Make sure that ePO server is properly installed before configuring VSE. For more information, see the McAfee ePO Product Documentation.

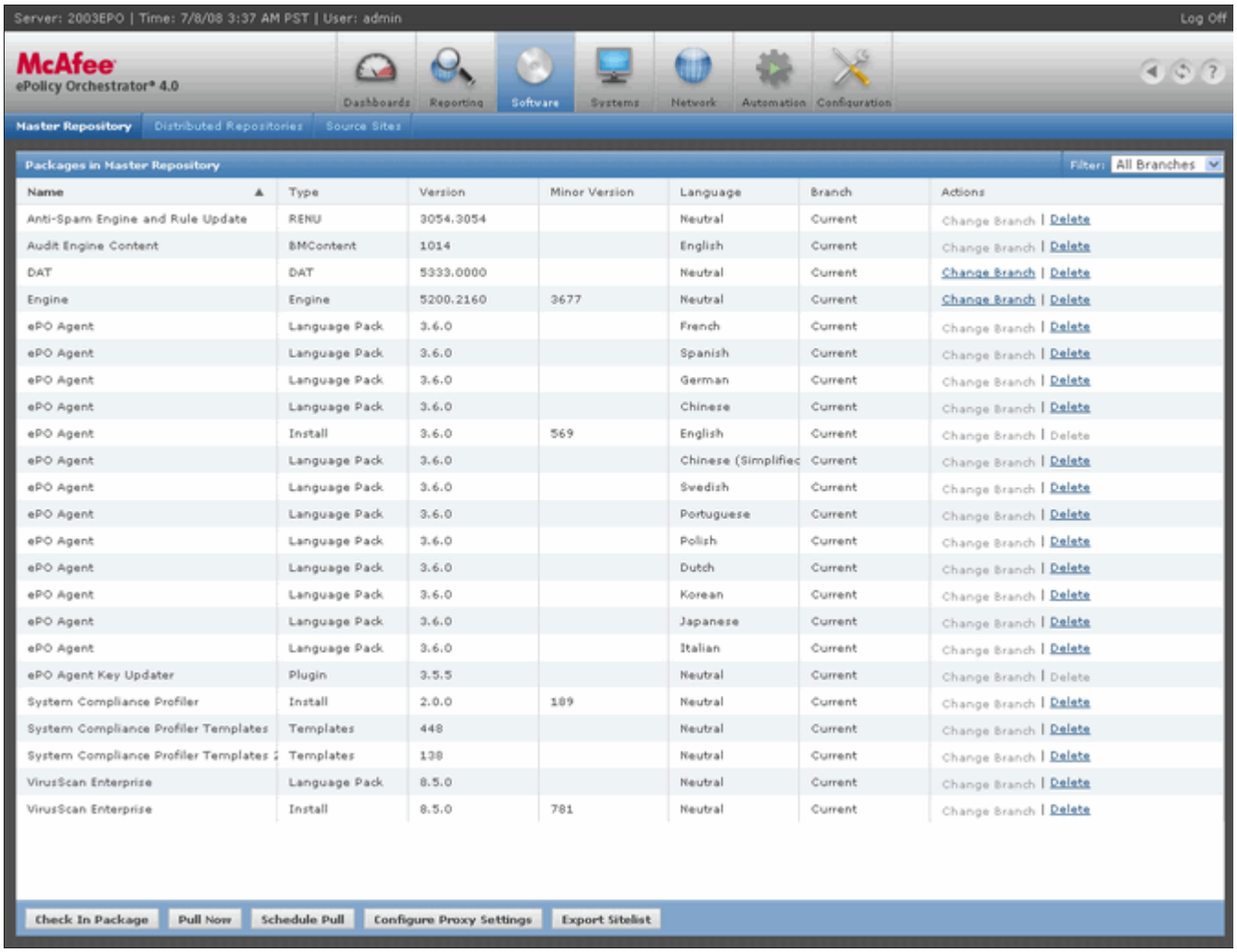
Configuring VSE Agents

To add the VSE install package to ePO server's Master Repository:

1. Download the VSE install package (e.g., `VSE85iENL.zip`) from McAfee.
2. Log in to the ePO Admin Console using a Web browser.
3. Click **Software**.
4. Make sure that **Master Repository** is selected.

   This is the default page displayed under **Software**.

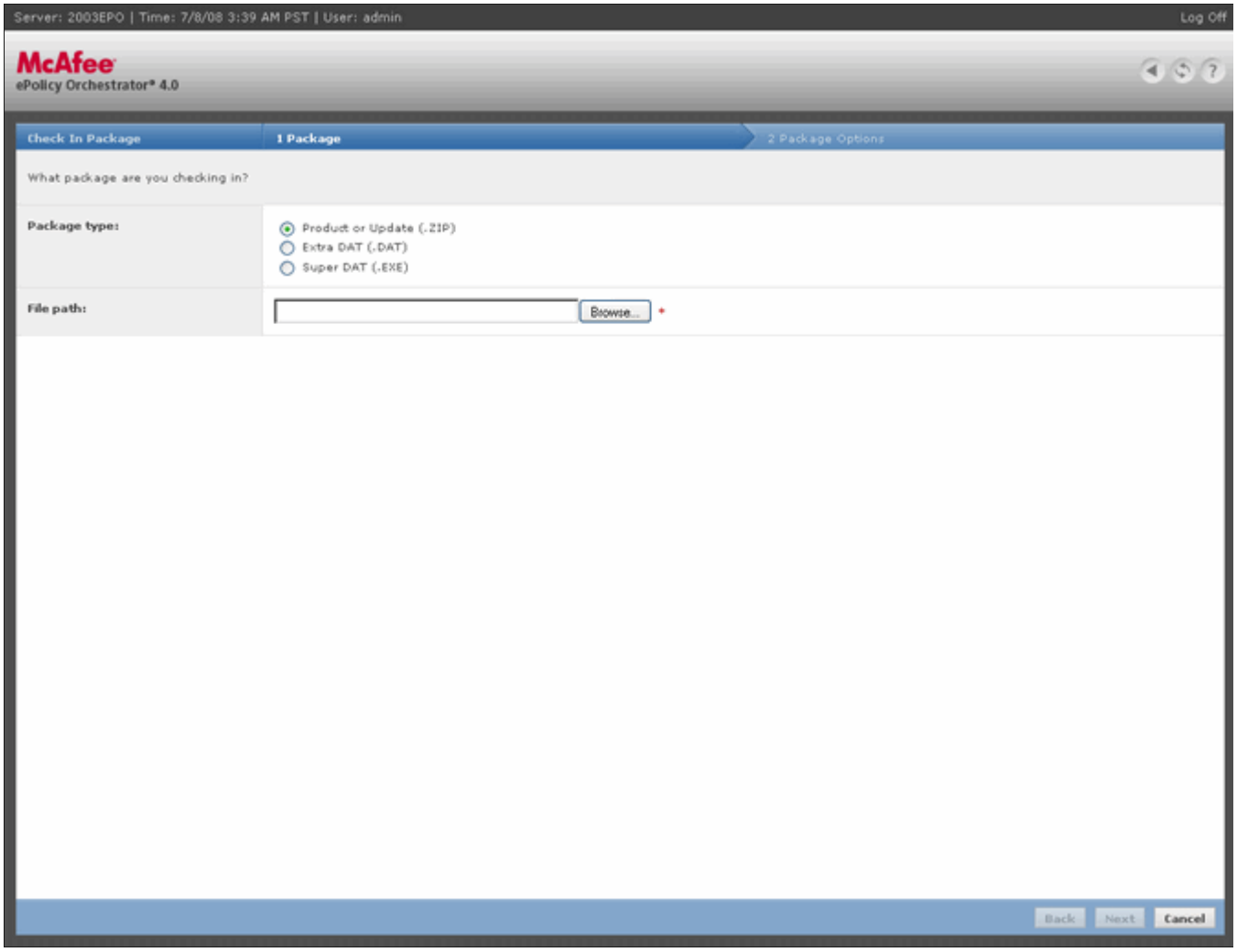
Figure 1 ePO Admin Console > Software > Master Repository


Server: 2003EPO | Time: 7/8/08 3:37 AM PST | User: admin
Log Off
McAfee
ePolicy Orchestrator® 4.0
Dashboards
Reporting
Software
Systems
Network
Automation
Configuration
Master Repository
Distributed Repositories
Source Sites
Packages in Master Repository
Filter: All Branches
Name
Type
Version
Minor Version
Language
Branch
Actions
Anti-Spam Engine and Rule Update | RENU | 3054.3054 | | Neutral | Current | Change Branch | Delete
Audit Engine Content | BMContent | 1014 | | English | Current | Change Branch | Delete
DAT | DAT | 5333.0000 | | Neutral | Current | Change Branch | Delete
Engine | Engine | 5200.2160 | 3677 | Neutral | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | French | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Spanish | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | German | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Chinese | Current | Change Branch | Delete
ePO Agent | Install | 3.6.0 | 569 | English | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Chinese (Simplifiec | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Swedish | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Portuguese | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Polish | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Dutch | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Korean | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Japanese | Current | Change Branch | Delete
ePO Agent | Language Pack | 3.6.0 | | Italian | Current | Change Branch | Delete
ePO Agent Key Updater | Plugin | 3.5.5 | | Neutral | Current | Change Branch | Delete
System Compliance Profiler | Install | 2.0.0 | 189 | Neutral | Current | Change Branch | Delete
System Compliance Profiler Templates | Templates | 448 | | Neutral | Current | Change Branch | Delete
System Compliance Profiler Templates | Templates | 138 | | Neutral | Current | Change Branch | Delete
VirusScan Enterprise | Language Pack | 8.5.0 | | Neutral | Current | Change Branch | Delete
VirusScan Enterprise | Install | 8.5.0 | 781 | Neutral | Current | Change Branch | Delete
Check In Package
Pull Now
Schedule Pull
Configure Proxy Settings
Export Sitelist

5. At the bottom of the page, click **Check In Package**.

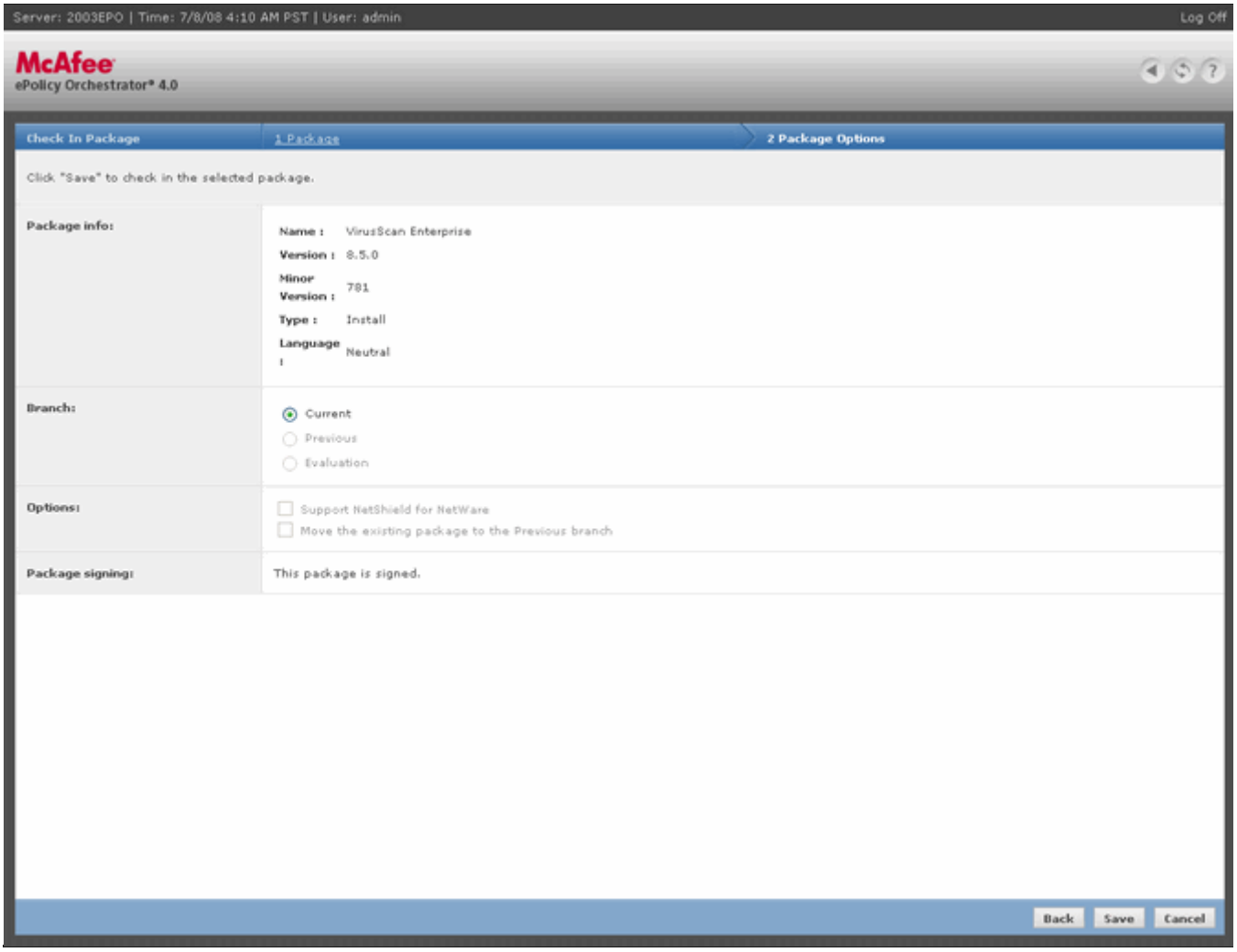
The **Check In Package** page appears.

Figure 2 Check In Package > 1 Package



6. On the **1 Package** page, for **Package Type** select the **Product or Update (.ZIP)** radio button.
7. For **File path**, click **Browse** and navigate to the location where the VSE install package (e.g., `VSE85iENL.zip`) is located.
8. At the bottom of the page, click **Next**.

Figure 3 Check In Package > 2 Package Options



9. On the **2 Package Options** page, for **Package Info** make sure that the information displayed is expected.
10. For **Branch**, make sure that the default option (e.g., **Current**) is selected.
11. Click **Save**.

To install the ePO Agent and VSE on ePO server:

> **IMPORTANT!** Make sure that you install an ePO Agent on every ePO server that has VSE installed. The ePO Agent is the application that facilitates all client/server communication and is responsible for pushing log data to the ePO server.

1. On the ePO server machine, install the ePO Agent (i.e., `FRAMEPKG.EXE`).

   By default, the ePO Agent installation package is located in the following directory on the ePO server:

   `C:\PROGRAM FILES\MCAFEE\EPO\DB\SOFTWARE\CURRENT\ePOAGENT3000\INSTALL\0409\FRAMEPKG.EXE`

Note: For detailed instructions regarding the ePO Agent installation, see the McAfee ePO 4.0 Product Documentation.

2. Install VSE.

   By default, the VSE installation package is located in the following directory on the ePO server:

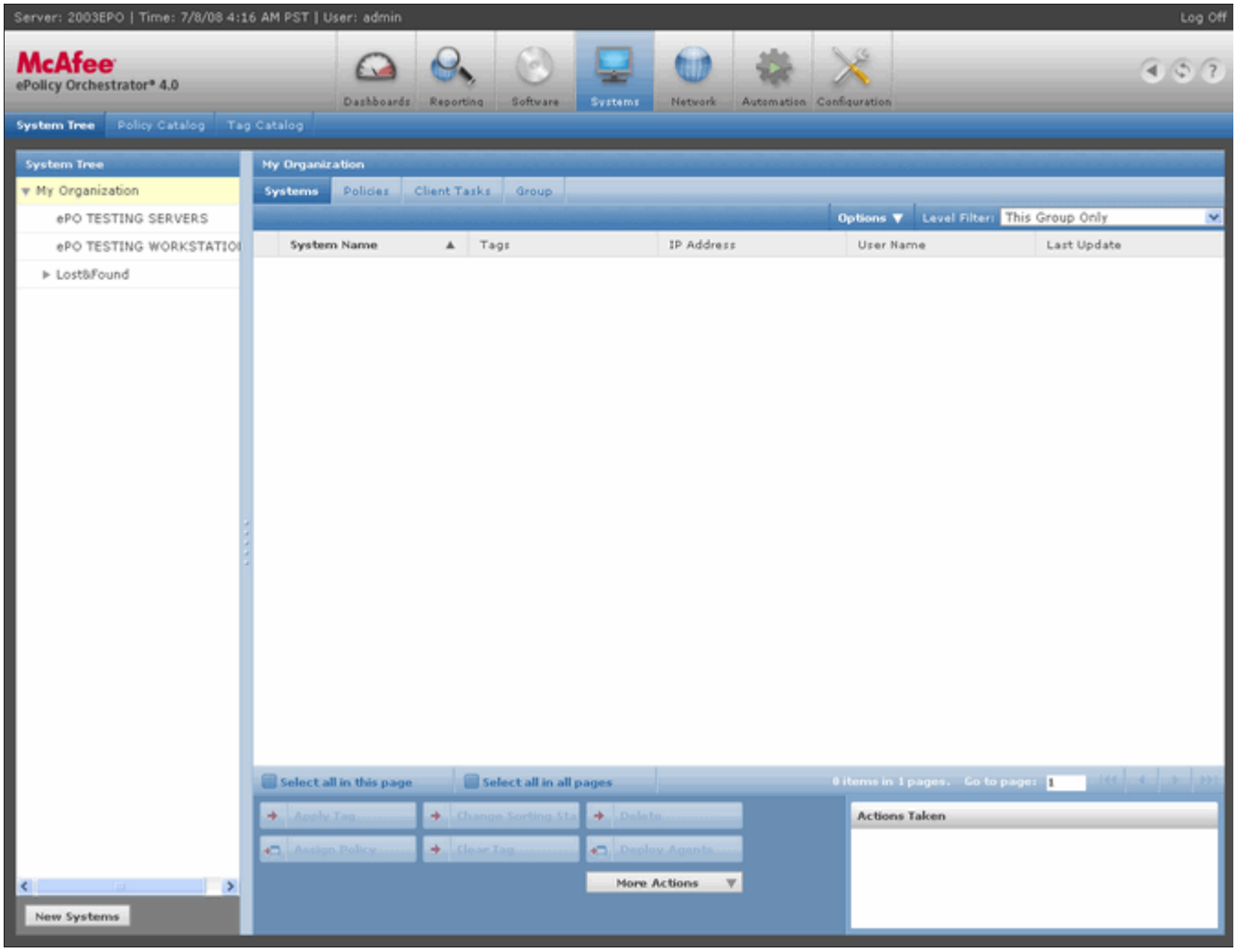
   ```
   C:\Program Files\McAfee\ePolicy
   Orchestrator\DB\Software\Current\VIRUSCAN8600
   ```

To configure a VSE policy for log file uploads on ePO server:

1. Log in to the ePO Admin Console using a Web browser.
2. Click **Systems**.
3. Make sure that **System Tree** is selected.

   This is the default page displayed under **Systems**.

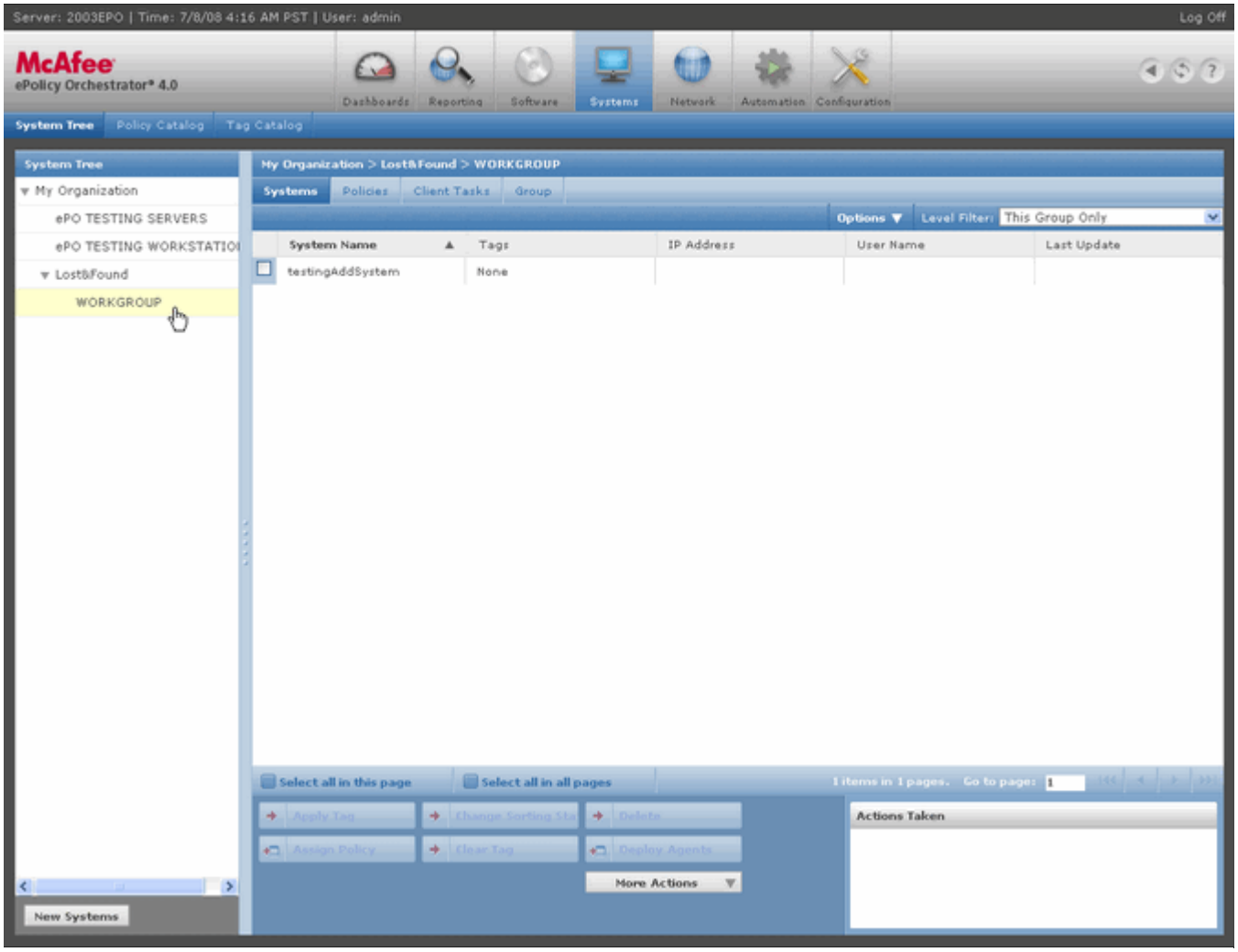
Figure 4 Systems > System Tree



4. Expand the **System Tree**, under **Lost&Found** within the tree select **WORKGROUP**.

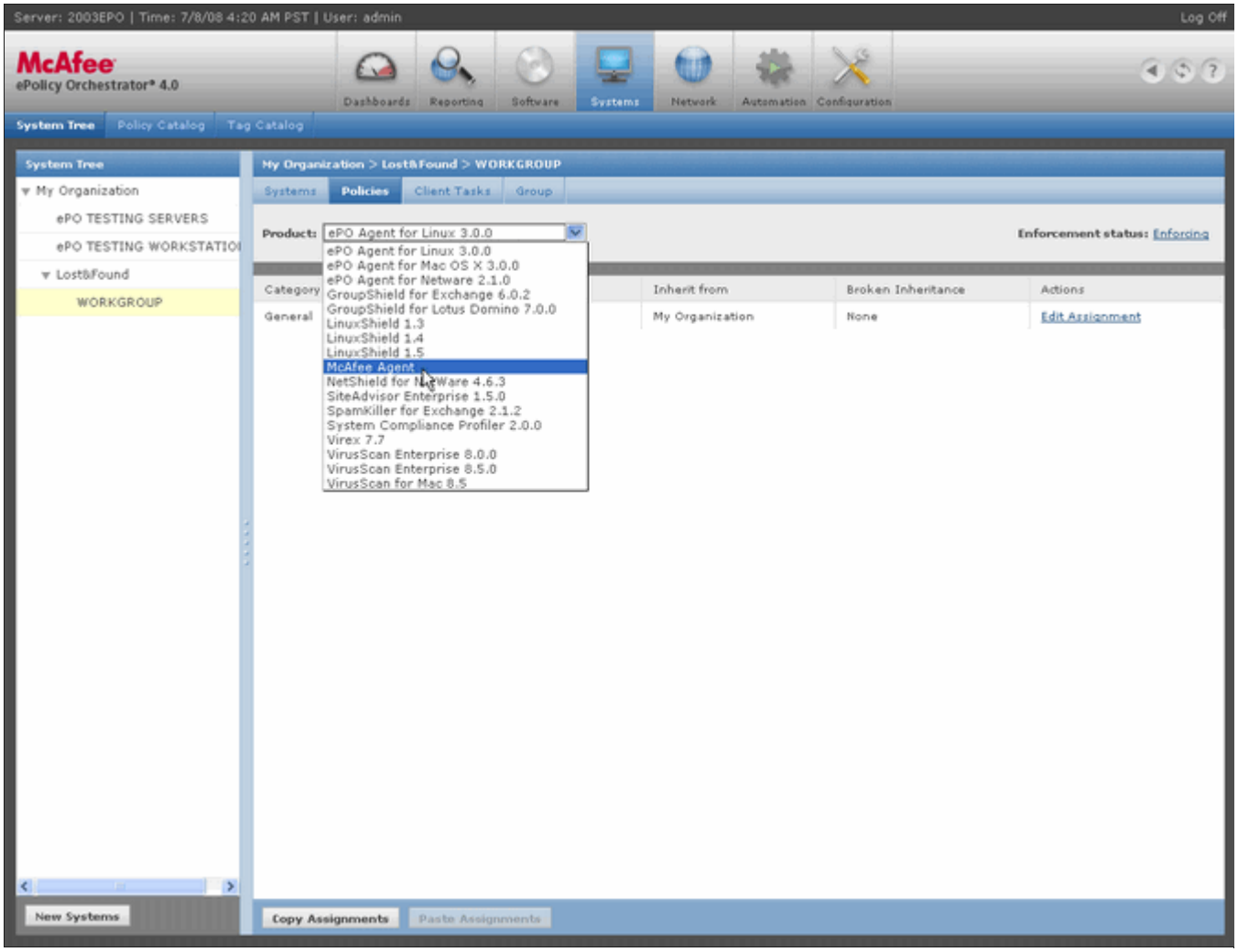
   WORKGROUP is the default group for agents.

Figure 5 System Tree > Lost&Found > WORKGROUP



5. In the right panel select **Policies**, then select **McAfee Agent** from the **Product** drop-down menu.

Figure 6 WORKGROUP > Policies > Product



6. Under the **Policy** column, click the **My Default** link.

   The **General** page appears for the agent.

7. For **General Options**, make sure that the following options are configured and enabled:

   - Set the **Policy enforcement interval (minutes)** option - The default is 5 minutes.
   - Make sure that the **Show the McAfee system tray icon (Windows only)** checkbox is selected.
   - Select the **Enable agent wake-up call support** checkbox.

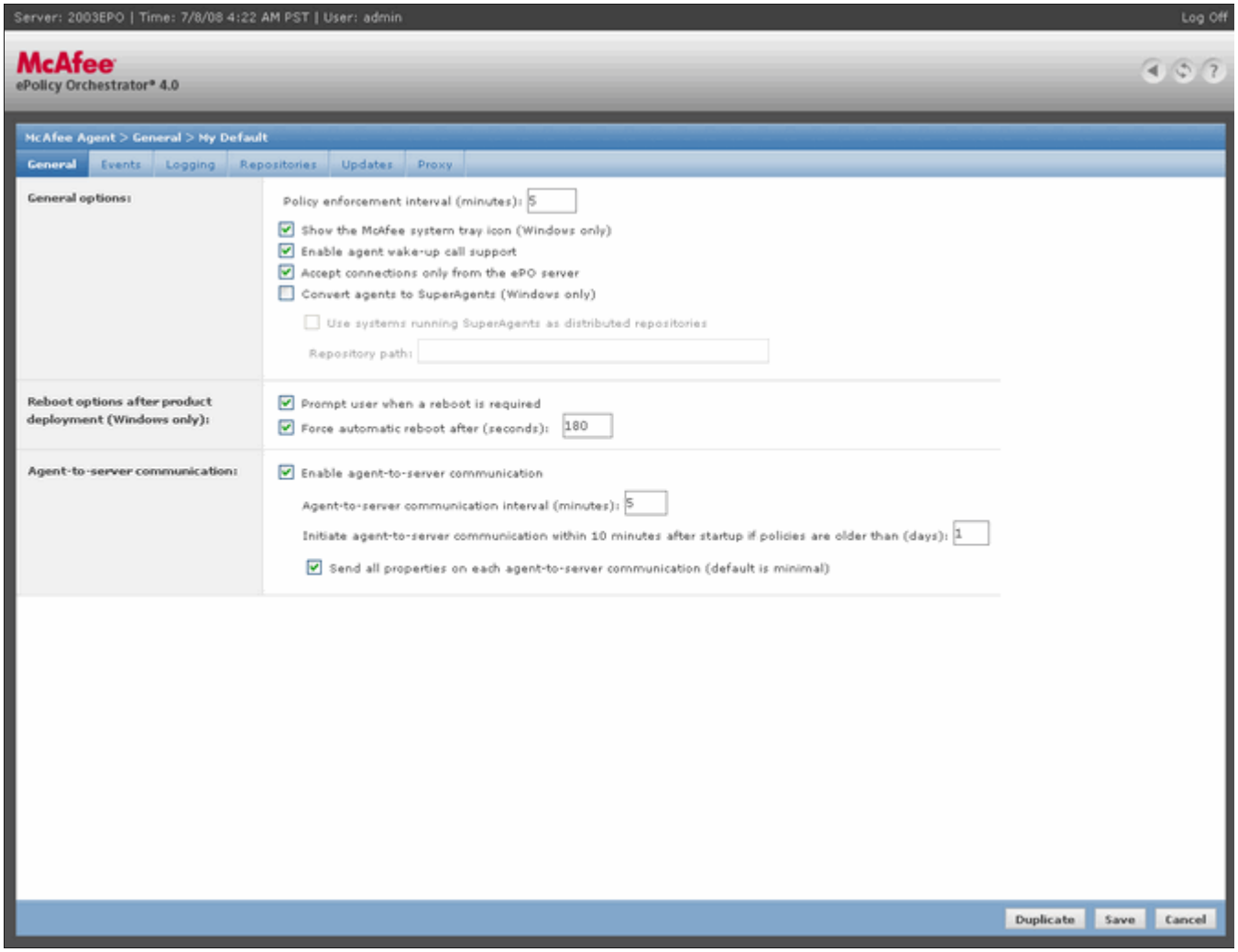
     This feature is disabled after the next agent-to-server communications interval. If you need this feature at a later time, you must wait an entire interval before it becomes available again.
   - Select the **Accept connections only from the ePO server** checkbox.

8. For **Reboot options after product deployment (Windows only)**, make sure that the following options are configured and enabled:

   - Make sure that the **Prompt user when a reboot is required checkbox** is selected.
   - Set the **Force automatic reboot after (seconds)** option - Set the option to 180 seconds. The default is 60 seconds.

9. For **Agent-to-server communication**, make sure that the following options are configured and enabled:
   - Make sure that the **Enable agent-to-server communication** checkbox is selected.
   - Set the **Agent-to-server communication interval (minutes)** option - Set the option to 5 minutes. The default is 60 minutes.
   - Set the **Initiate agent-to-server communication within 10 minutes after startup if policies are older than (days)** - The default is 1 day.
   - Make sure that the **Send all properties on each agent-to-server communication (default is minimal)** checkbox is selected.

Figure 7 My Default > General

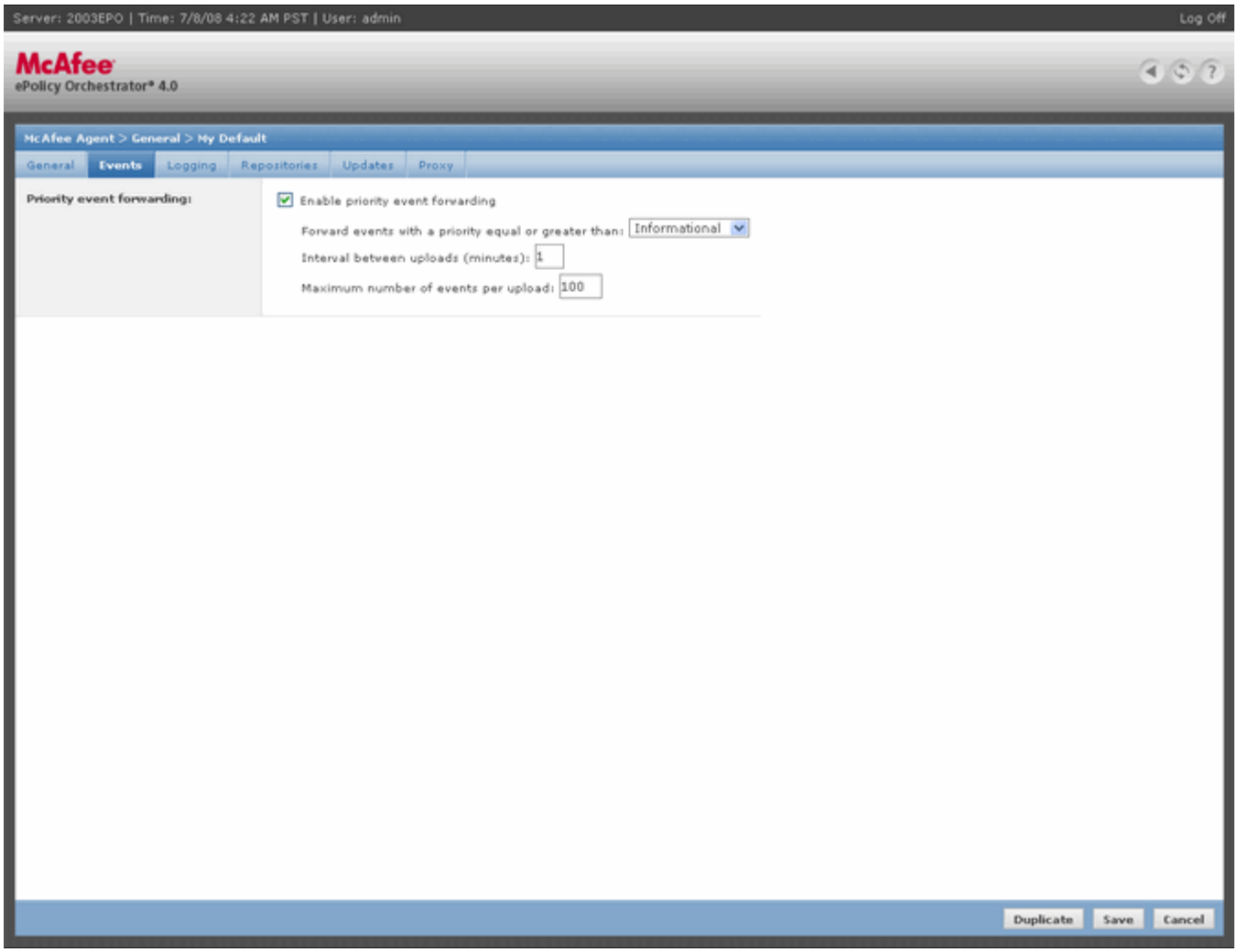

Server: 2003EPO | Time: 7/8/08 4:22 AM PST | User: admin
Log Off
McAfee
ePolicy Orchestrator® 4.0
McAfee Agent > General > My Default
General
Events
Logging
Repositories
Updates
Proxy
General options:
Policy enforcement interval (minutes): 5
Show the McAfee system tray icon (Windows only)
Enable agent wake-up call support
Accept connections only from the ePO server
Convert agents to SuperAgents (Windows only)
Use systems running SuperAgents as distributed repositories
Repository path:
Reboot options after product deployment (Windows only):
Prompt user when a reboot is required
Force automatic reboot after (seconds): 180
Agent-to-server communication:
Enable agent-to-server communication
Agent-to-server communication interval (minutes): 5
Initiate agent-to-server communication within 10 minutes after startup if policies are older than (days): 1
Send all properties on each agent-to-server communication (default is minimal)
Duplicate
Save
Cancel

10. Click **Events**.

    The **Events** page appears for the agent.

11. For **Priority event forwarding**, make sure that the following options are configured and enabled:
    - Make sure that the **Enable priority event forwarding** checkbox is selected.
    - From the **Forward events with a priority equal or greater than** drop-down menu select **Informational**.
    - Set the **Interval between uploads (minutes)** option - Set to 1 minute. The default is 5 minutes.
    - Set the **Maximum number of events per upload** option - Set to 100 events. The default is 10 events.

Figure 8 My Default > Events

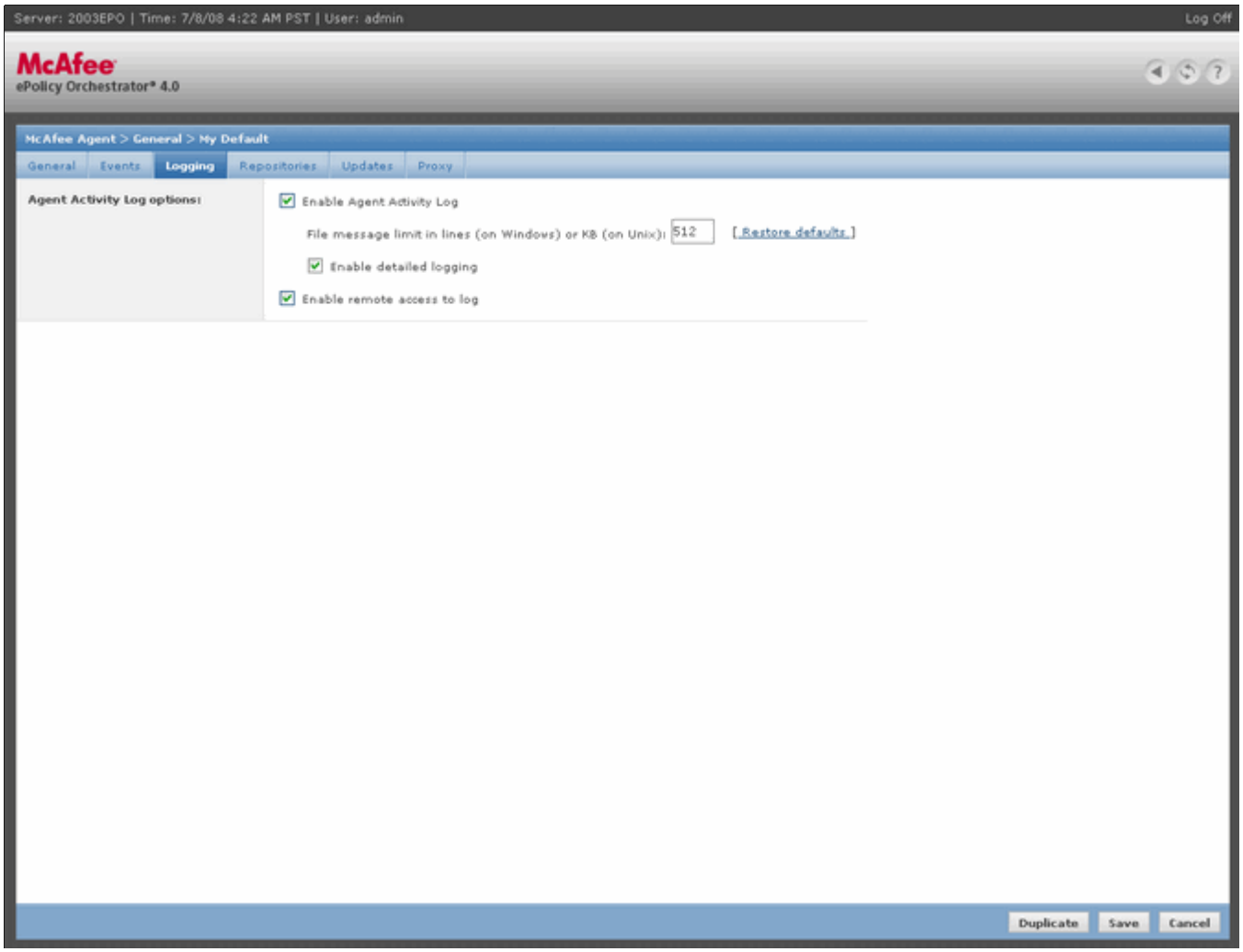


12. Click **Logging**.

    The **Logging** page appears for the agent.

13. For **Agent Activity Log options**, make sure that the following options are configured and enabled:
    - Make sure that the **Enable Agent Activity Log** checkbox is selected.
    - Set the **File message limit in lines (on Windows) or KB (on Unix)** option - Set to 512 lines. The default is 200 lines.
    - Select the **Enable detailed logging** checkbox.
    - Make sure that the **Enable remote access to log** checkbox is selected.

Figure 9 My Default > Logging



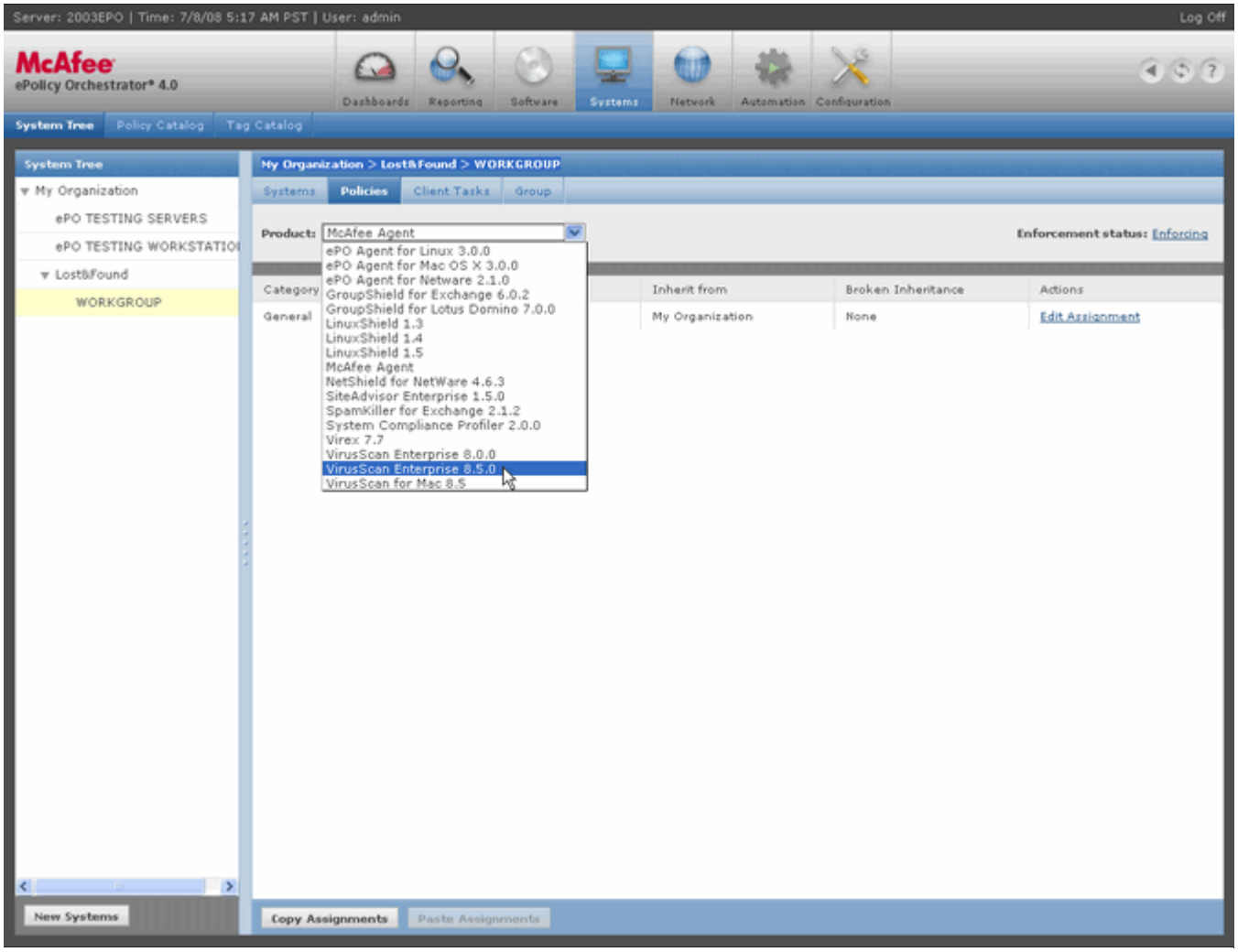
14. Click **Save**.

    Keep the default selections for the **Repositories**, **Updates**, and **Proxy** pages.

15. Return to the **My Organization > Lost&Found > WORKGROUP > Policies** page.

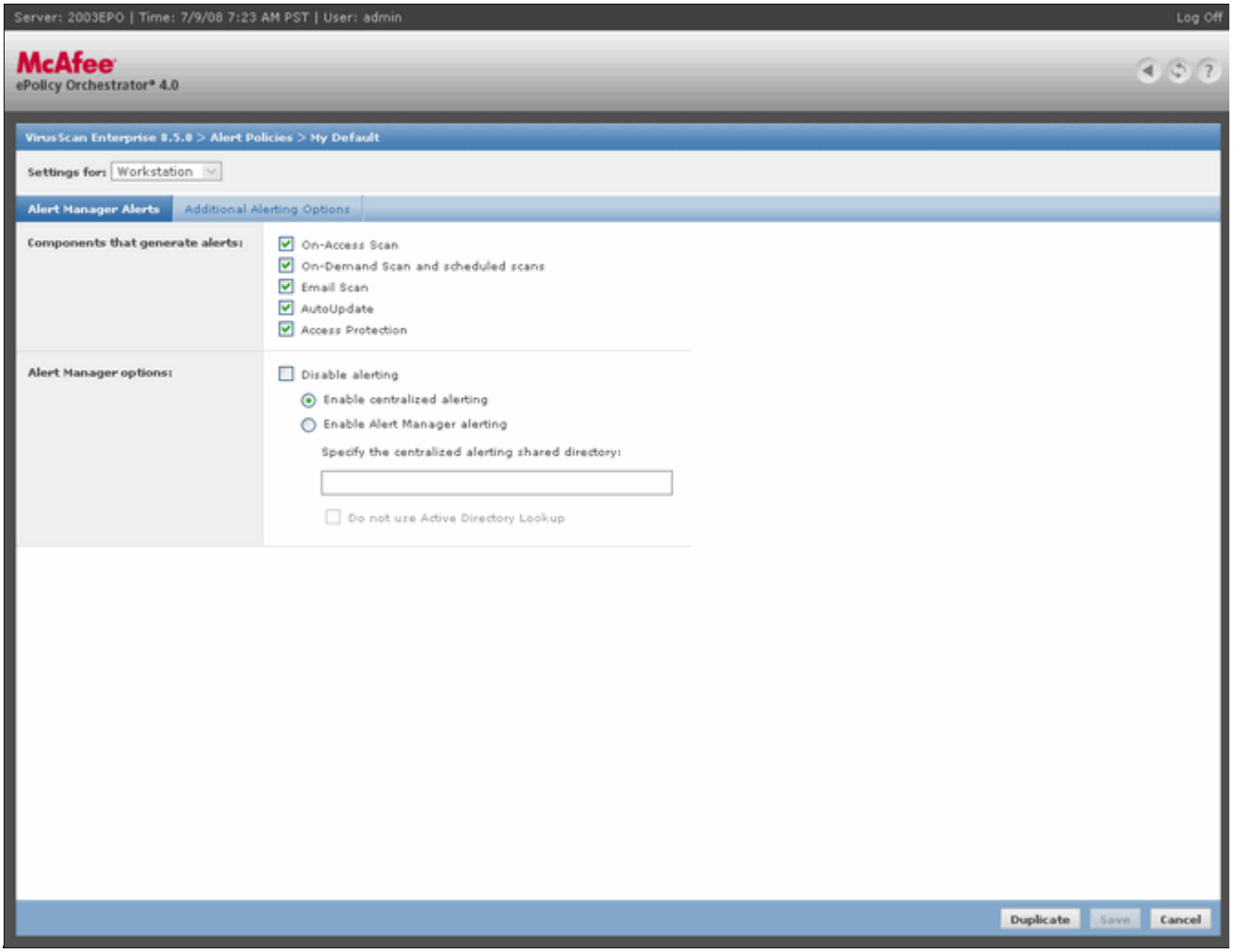
16. Select **VirusScan Enterprise 8.5** from the **Product** drop-down menu.

Figure 10 WORKGROUP > Policies > Product



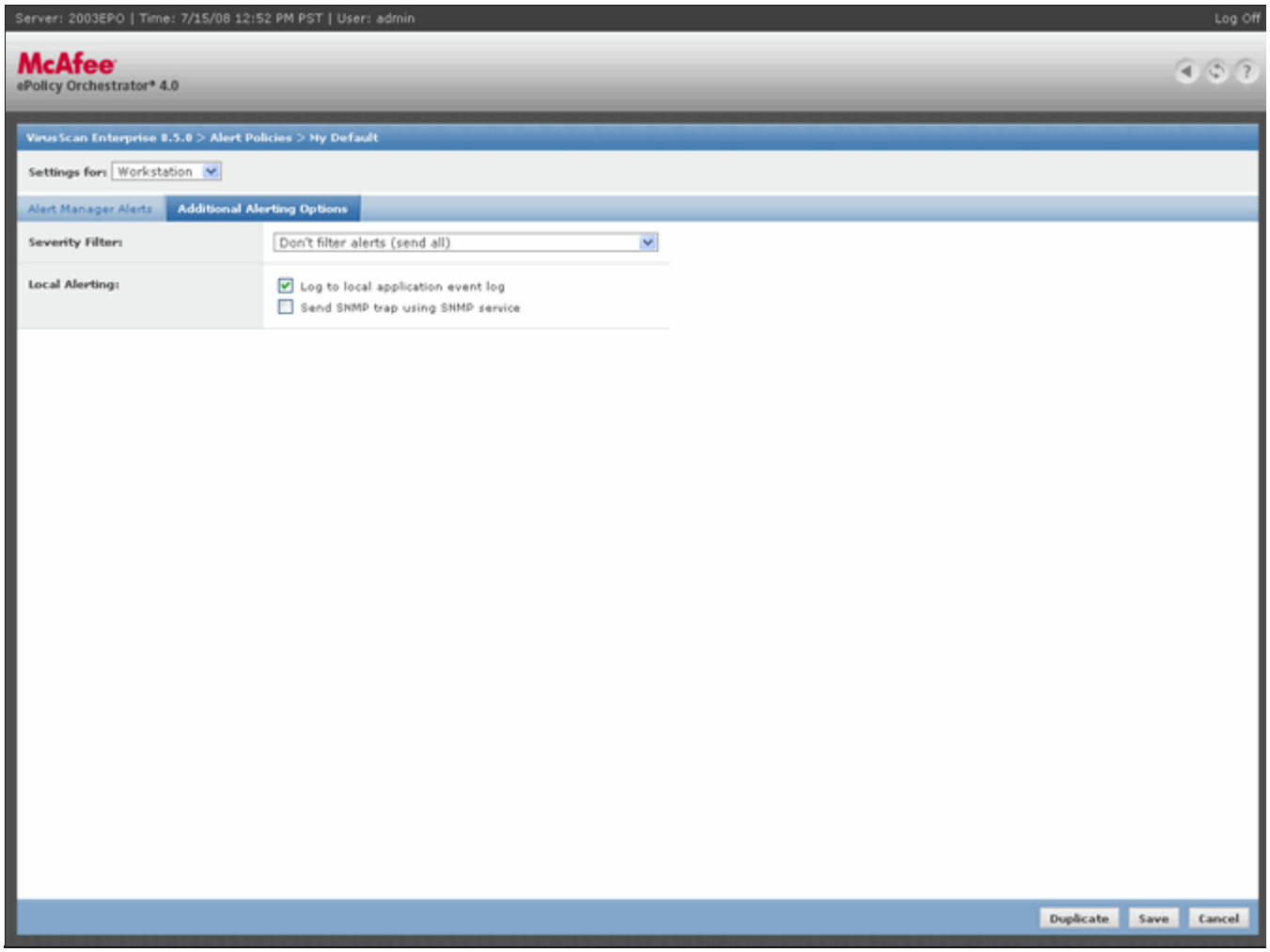
17. Under the **Policy** column, for **Alert Policies** click the **My Default** link.
18. From the **Settings for** drop-down menu, make sure that **Workstation** or **Server** is selected depending on your environment.
19. On the **Alert Manager Alerts** page, for the **Components that generate alerts** section, select all of the checkboxes to enable all alerts.
20. For the **Alert Manager options** section, select the **Enable centralized alerting** radio button.

Figure 11 Alert Policies > My Default > Alert Manager Alerts



21. Click **Additional Alerting Options** to display that page.
22. For **Severity Filter**, select **Don't filter alerts (send all)** from the drop-down menu.
23. For **Local Alerting**, select the **Log to local application event log** checkbox.

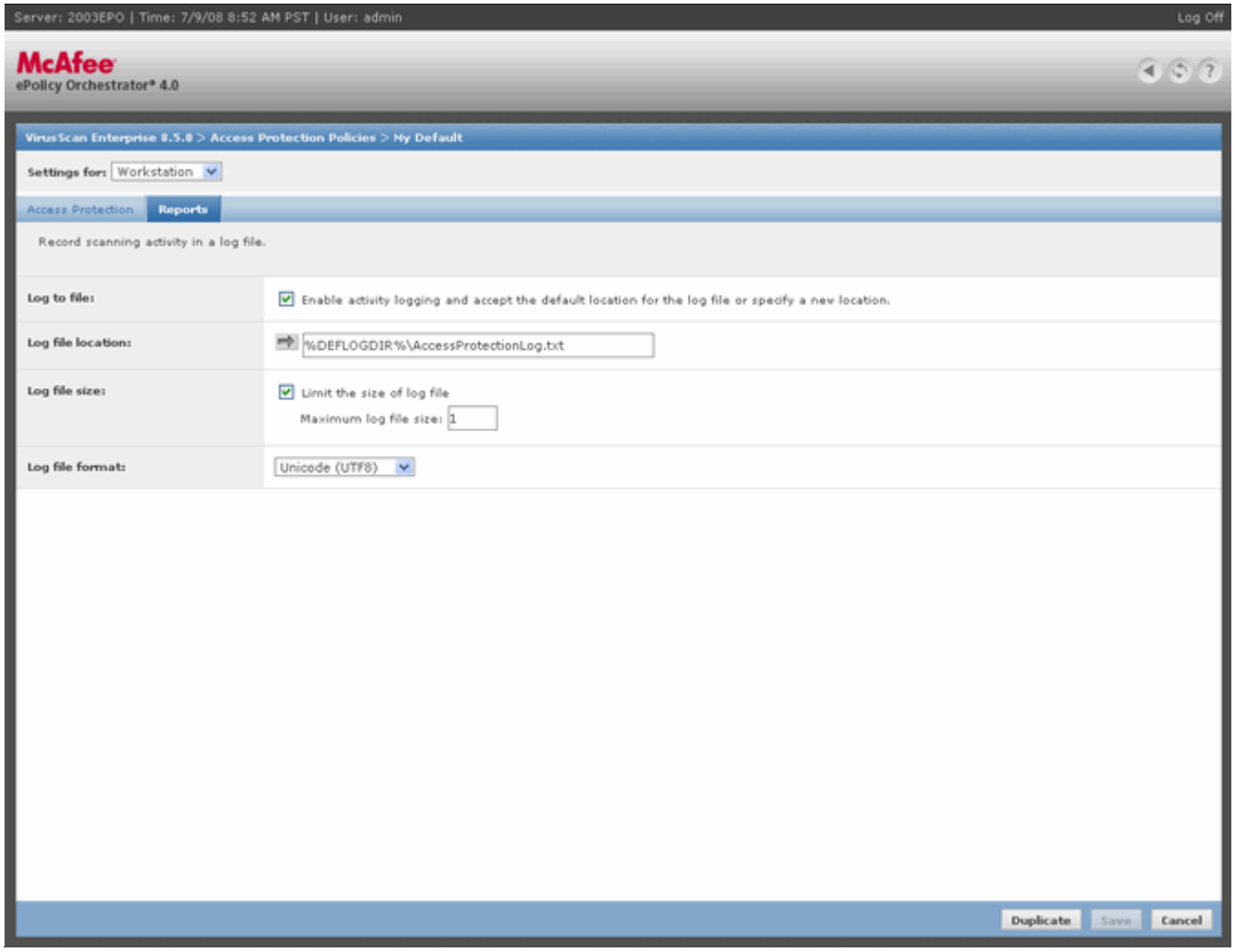
Figure 12 Alert Polices > My Default > Additional Alerting Options



24. Click **Save**.
25. Return to the **My Organization > Lost&Found > WORKGROUP > Policies** page.
26. For each of the following categories, edit the **My Default > Reports** options to enable and configure reporting depending on your environment:
    - Access Protection Policies
    - Buffer Overflow Protection Policies
    - On-Access Default Processes Policies
    - On-Access General Policies
    - On-Access High-Risk Processes Policies
    - On-Access Low-Risk Processes Policies
    - On Delivery Email Scan Policies

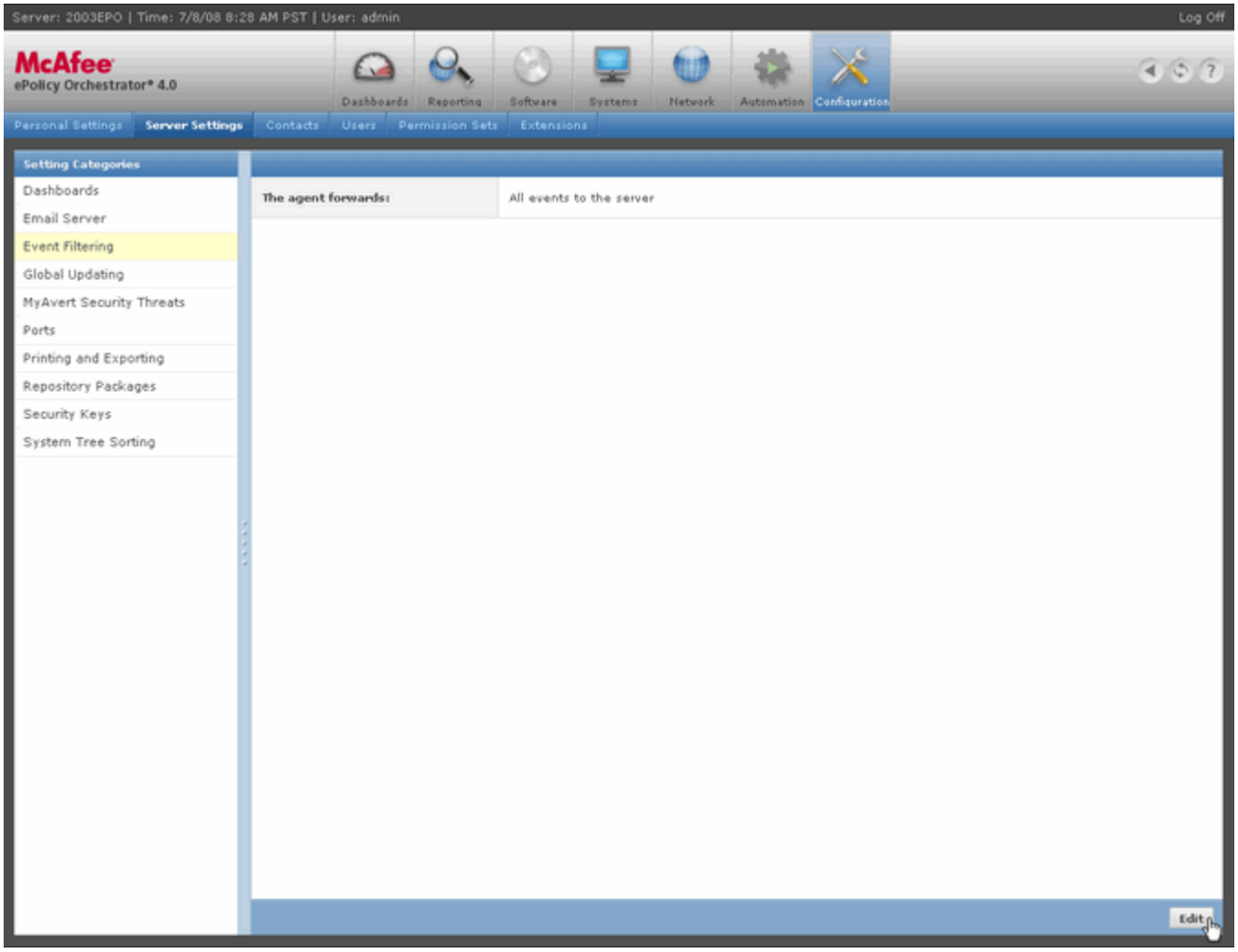
Note: For more information regarding the various **Reports** page options, see the McAfee ePO Product Documentation.

Figure 13 Access Protection Policies > My Default > Reports


Server: 2003EPO | Time: 7/9/08 8:52 AM PST | User: admin
Log Off
McAfee
ePolicy Orchestrator® 4.0
VirusScan Enterprise 8.5.0 > Access Protection Policies > My Default
Settings for: Workstation
Access Protection
Reports
Record scanning activity in a log file.
Log to file:
Enable activity logging and accept the default location for the log file or specify a new location.
Log file location:
%DEFLOGDIR%\AccessProtectionLog.txt
Log file size:
Limit the size of log file
Maximum log file size: 1
Log file format:
Unicode (UTF8)
Duplicate
Save
Cancel

27. Click **Configuration** > **Server Settings**.

Figure 14 ePO Admin Console > Configuration > Server Settings

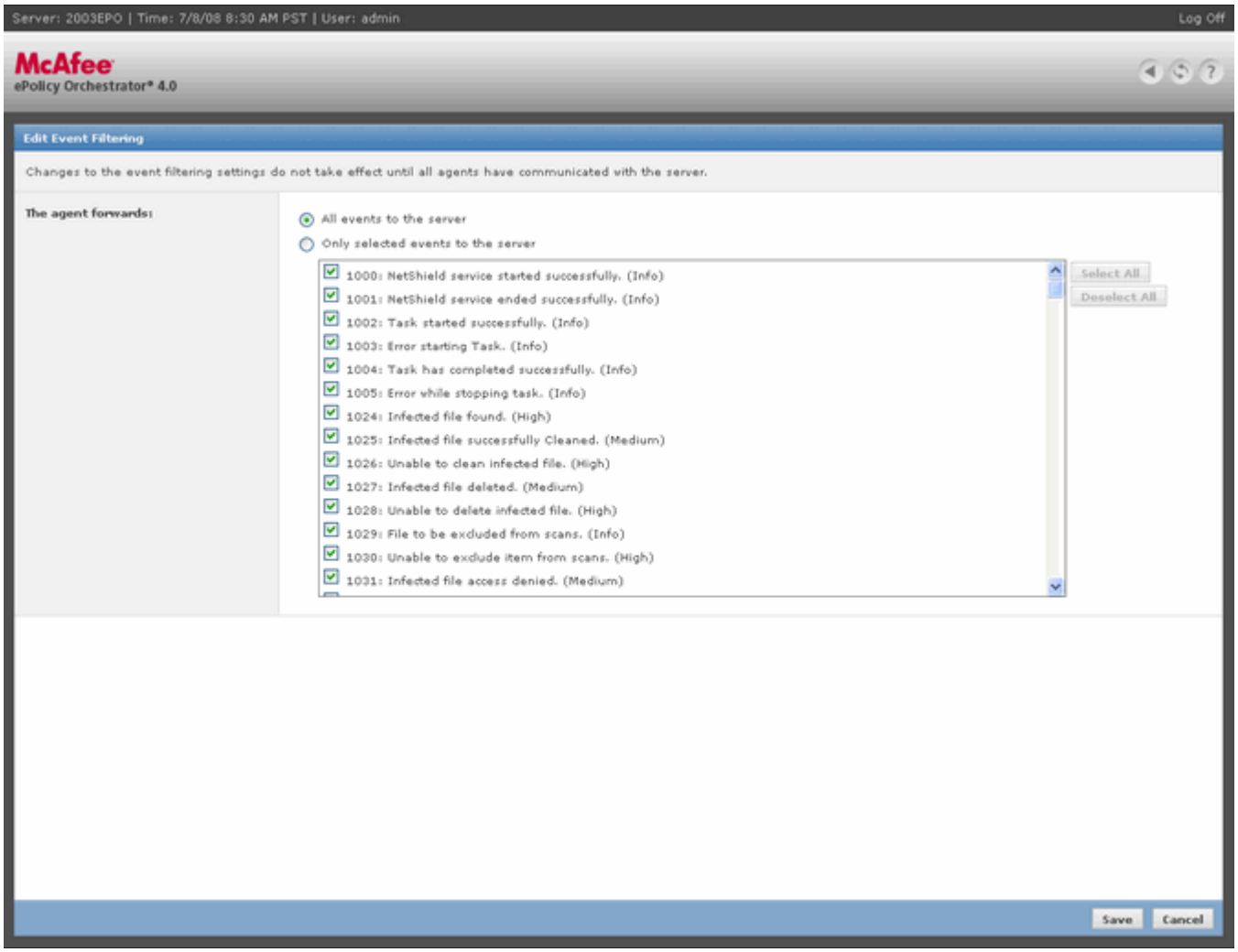


28. Select **Event Filtering**, then click **Edit**.

    The **Edit Event Filtering** page appears.

29. For **The agent forwards** option, select the **All events to the server** radio button.

Figure 15 Event Filtering > Edit Event Filtering


Server: 2003EPO | Time: 7/8/08 8:30 AM PST | User: admin
Log Off
McAfee
ePolicy Orchestrator® 4.0
Edit Event Filtering
Changes to the event filtering settings do not take effect until all agents have communicated with the server.
The agent forwards:
All events to the server
Only selected events to the server
1000: NetShield service started successfully. (Info)
1001: NetShield service ended successfully. (Info)
1002: Task started successfully. (Info)
1003: Error starting Task. (Info)
1004: Task has completed successfully. (Info)
1005: Error while stopping task. (Info)
1024: Infected file found. (High)
1025: Infected file successfully Cleaned. (Medium)
1026: Unable to clean infected file. (High)
1027: Infected file deleted. (Medium)
1028: Unable to delete infected file. (High)
1029: File to be excluded from scans. (Info)
1030: Unable to exclude item from scans. (High)
1031: Infected file access denied. (Medium)
Select All
Deselect All
Save
Cancel

30. Click **Save**.

Enabling the LogLogic Appliance to Capture Log Data

The following sections describe how to enable the LogLogic Appliance to capture McAfee ePO log data.

Adding a McAfee ePO Device

The LogLogic Database Collector is a base component of the LogLogic Appliance that connects to McAfee ePO and retrieves the VSE log information. You must add the server as a new device so LogLogic can properly handle the log file data to make it available through reports and searching.

To add McAfee ePO as a new device

1. Log in to the LogLogic Appliance.

2. From the navigation menu, select **Management > Devices**.

The **Devices** tab appears.

3. Click **Add New**.

   The **Add Device** tab appears.

4. Type in the following information for the device:

   - **Name**—Name for the McAfee ePO device
   - **Description** (optional)—Description of the McAfee ePO device
   - **Device Type**—Select McAfee ePO from the drop-down menu
   - **Host IP**—IP address of the McAfee ePO appliance
   - **Enable Data Collection**—Select the **Yes** radio button
   - **Refresh Device Name through DNS Lookups** (optional)—Select this checkbox to enable the **Name** field to be automatically updated. The name is obtained using a reverse DNS lookup on the configured refresh interval. The DNS name overrides any manual name you assign.

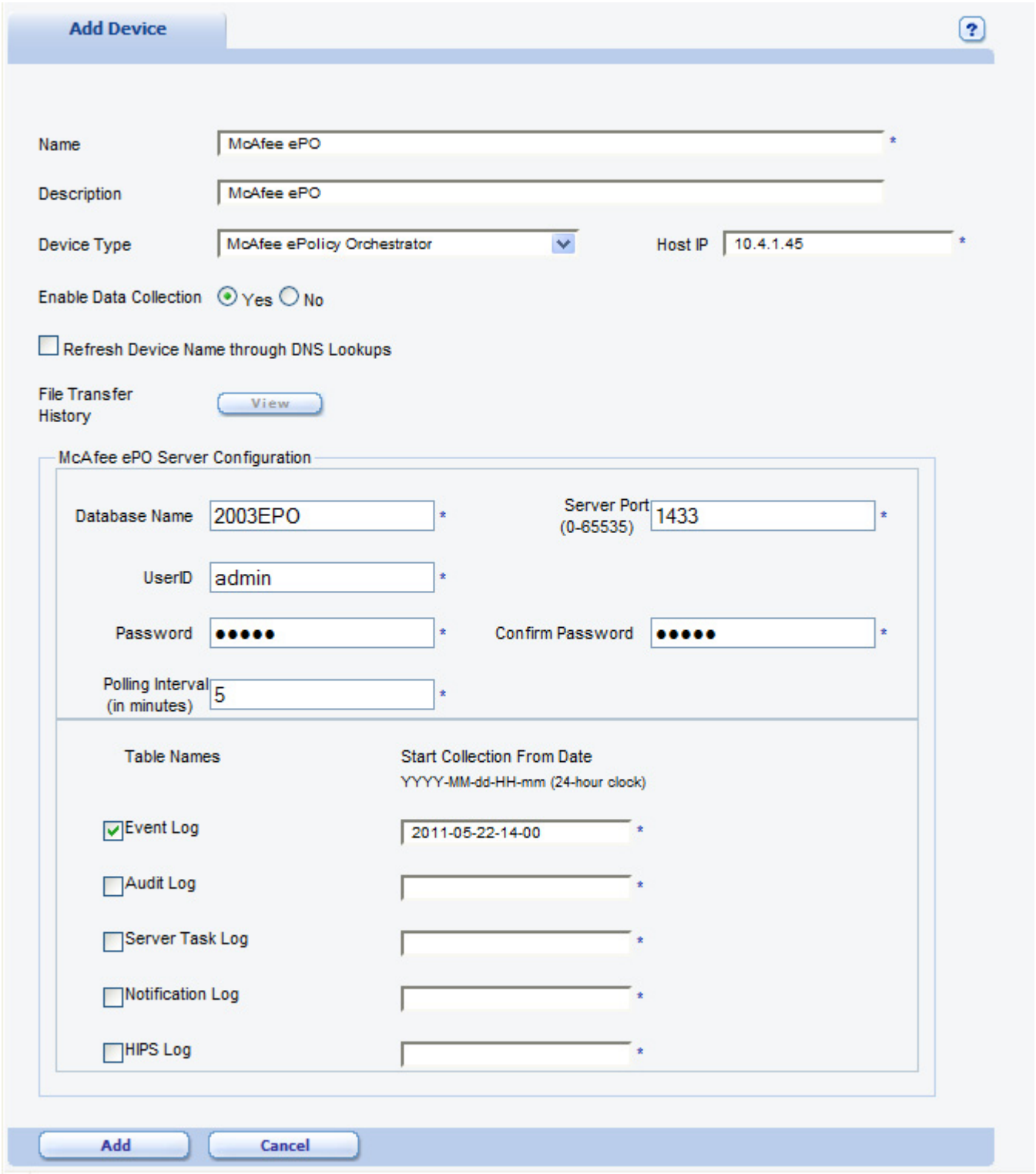
5. Under the McAfee ePO **Server Configuration** section, configure the following options:

   - **Database Name**—McAfee ePO database instance name
   - **Server Port**—Port number for McAfee ePO
   - **UserID**—User name for the database user
   - **Password/Confirm Password**—Password for the database user
   - **Polling Interval**—The default value for the polling interval is 5 minutes
   - Select the checkbox for any of the following log types:
     - **Event Log**—This checkbox is selected by default
     - **Audit Log**
     - **Server Task Log**
     - **Notification Log**
     - **HIPS Log**

     For more information on each log, see *How LogLogic Captures McAfee ePO Log Data* on page 28.
   - **Start Collection From Date**—For each selected log type, specify the date and time that the LogLogic Appliance will begin to collect log data

6. Click **Add**.

Figure 16 Adding a Device to the LogLogic Appliance



7. Verify that your new device appears in the **Devices** tab and that **Enabled** is set to **Yes**.

   When the logs arrive from the specified McAfee ePO, the LogLogic Appliance uses the device you just added if the IP address matches.

Testing Connectivity

After configuring McAfee ePO and the LogLogic Appliance, you should test the connectivity between the ePO server's database and the Appliance.

To test connectivity:

1. Log in to the LogLogic Appliance.
2. From the navigation menu, select **Management > Devices**.

   The **Devices** tab appears.
3. Select the name of the McAfee ePO device you want to test.

   The **Modify Device** tab appears.
4. Click **Test**.

If the connection fails, an error displays and in some cases a potential diagnosis. Also, the number of eligible log records to be collected is displayed.

Verifying the Configuration

The section describes how to verify that the configuration changes made to McAfee ePO and the LogLogic Appliance are applied correctly.

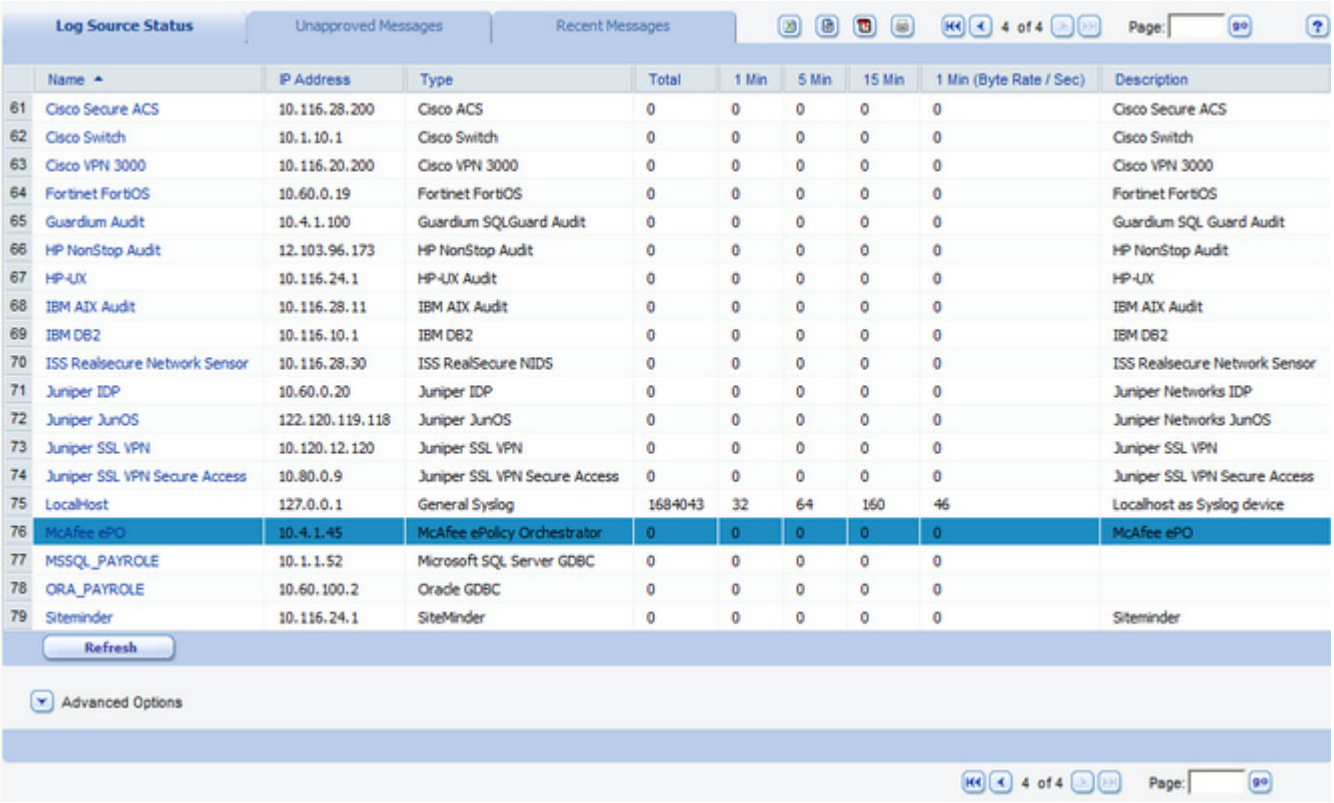
To verify the configuration:

1. Log in to the LogLogic Appliance.
2. From the navigation menu, select **Dashboards > Log Source Status**.

   The **Log Source Status** tab appears.
3. Locate the IP address for each McAfee ePO device.

If the device name (**McAfee ePO**) appears in the list of devices, then the configuration is correct (see Figure 17 on page 27).

Figure 17 Verification of the McAfee ePO Configuration



Log Source Status | Unapproved Messages | Recent Messages | 4 of 4 | Page:

	Name	IP Address	Type	Total	1 Min	5 Min	15 Min	1 Min (Byte Rate / Sec)	Description
61	Cisco Secure ACS	10.116.28.200	Cisco ACS	0	0	0	0	0	Cisco Secure ACS
62	Cisco Switch	10.1.10.1	Cisco Switch	0	0	0	0	0	Cisco Switch
63	Cisco VPN 3000	10.116.20.200	Cisco VPN 3000	0	0	0	0	0	Cisco VPN 3000
64	Fortinet FortiOS	10.60.0.19	Fortinet FortiOS	0	0	0	0	0	Fortinet FortiOS
65	Guardium Audit	10.4.1.100	Guardium SQLGuard Audit	0	0	0	0	0	Guardium SQL Guard Audit
66	HP NonStop Audit	12.103.96.173	HP NonStop Audit	0	0	0	0	0	HP NonStop Audit
67	HP-UX	10.116.24.1	HP-UX Audit	0	0	0	0	0	HP-UX
68	IBM AIX Audit	10.116.28.11	IBM AIX Audit	0	0	0	0	0	IBM AIX Audit
69	IBM DB2	10.116.10.1	IBM DB2	0	0	0	0	0	IBM DB2
70	ISS Realsecure Network Sensor	10.116.28.30	ISS RealSecure NIDS	0	0	0	0	0	ISS Realsecure Network Sensor
71	Juniper IDP	10.60.0.20	Juniper IDP	0	0	0	0	0	Juniper Networks IDP
72	Juniper JunOS	122.120.119.118	Juniper JunOS	0	0	0	0	0	Juniper Networks JunOS
73	Juniper SSL VPN	10.120.12.120	Juniper SSL VPN	0	0	0	0	0	Juniper SSL VPN
74	Juniper SSL VPN Secure Access	10.80.0.9	Juniper SSL VPN Secure Access	0	0	0	0	0	Juniper SSL VPN Secure Access
75	LocalHost	127.0.0.1	General Syslog	1684043	32	64	160	46	Localhost as Syslog device
76	McAfee ePO	10.4.1.45	McAfee ePolicy Orchestrator	0	0	0	0	0	McAfee ePO
77	MSSQL_PAYROLE	10.1.1.52	Microsoft SQL Server GDBC	0	0	0	0	0	
78	ORA_PAYROLE	10.60.100.2	Oracle GDBC	0	0	0	0	0	
79	Siteminder	10.116.24.1	SiteMinder	0	0	0	0	0	Siteminder

Refresh

Advanced Options

4 of 4 | Page:

If the device does not appear in the **Log Source Status** tab, check the McAfee ePO logs for events that should have been sent. If events were detected and are still not appearing on the LogLogic Appliance, verify the McAfee ePO configuration, and the LogLogic Appliance configuration.

You can also verify that the LogLogic Appliance is properly capturing log data from McAfee ePO by trying to view the data in the reports. LogLogic recommends checking the reports to make sure that the data obtained is valid and matches expectations. For more information, see *LogLogic Real-Time Reports* on page 29.

If the device name appears in the list of devices but log data for the device is not appearing within your reports, you need to verify that your database connection is up and running properly. For more information, see *Testing Connectivity* on page 26 and *Troubleshooting* on page 35.

Note: It takes approximately 5 minutes for file pulling to begin. Wait at least 5 minutes for the log data to appear before testing the connectivity or going through troubleshooting efforts.

Chapter 2 – How LogLogic Supports McAfee ePO

This chapter describes LogLogic's support for McAfee ePO. LogLogic enables you to capture log data to monitor McAfee ePO events.

- How LogLogic Captures McAfee ePO Log Data 28
- LogLogic Real-Time Reports. 29
- LogLogic Search Filters. 32

How LogLogic Captures McAfee ePO Log Data

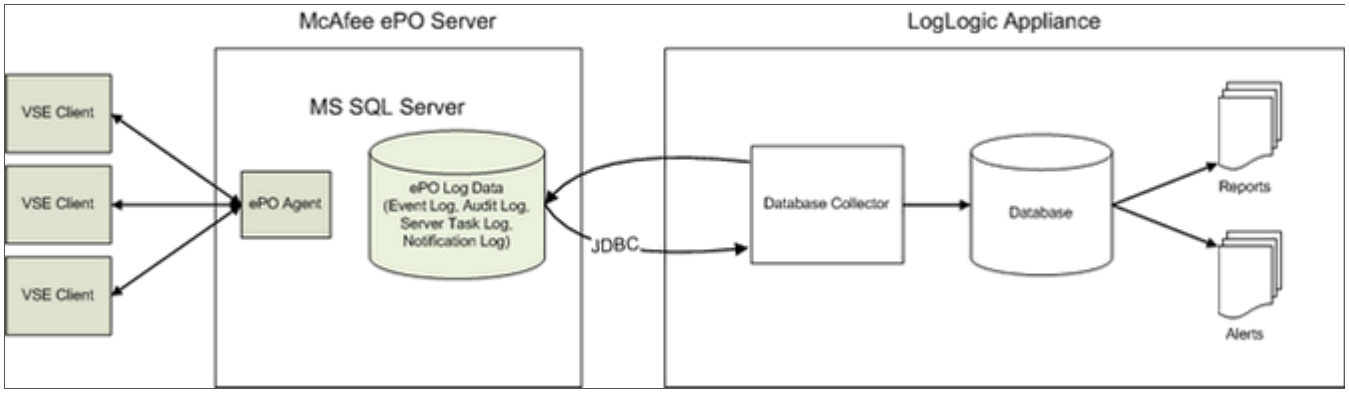
McAfee ePO is a Windows-based application that uses Microsoft SQL Server to store all policy, server log, and VSE client log information. McAfee's ePO Agent is installed on all VSE client systems. The ePO Agent facilitates all VSE client to ePO server communication and is responsible for pushing log data from the VSE clients to the ePO server. LogLogic's Database Collector connects to ePO's Microsoft SQL Server database via JDBC to capture the log data. The Database Collector obtains information for the following logs:

- Event Log—Information is collected from the EPOEvents table within the ePO database. This log contains information for all of the following VSE client logs:
  - Access Protection Logs
  - Buffer Overflow Protection Logs
  - (Email Scan) Email on Delivery Logs
  - Update Logs
  - On Access Scan Logs
  - (Full Scan) On Demand Scan Logs
- Audit Log—Information is collected from the OrionAuditLog table within the ePO database. This log contains information that provides accountability in the network environment, such as:
  - User login
  - Adding or deleting a group
  - Adding or deleting a user
  - Adding or deleting a computer
  - User role change
  - Uninstalling an agent when deleting
  - User password change
  - Renaming sites, groups, or computers
  - Adding or deleting a site
  - Policy changes

- Server Task Log—Information is collected from the OrionSchedulerTaskLog table within the ePO database. This log contains data about all ePO server maintenance tasks, such as live update retrieval, report generation, etc.
- Notification Log—Information is collected from the EPONotificationLog table within the ePO database. This log captures all SNMP and email notification events that are sent from ePO server.

> **Note:** McAfee ePO also supports Windows Event Log information. Windows Event Log information can be collected using LogLogic's Windows Event Collector, Lasso. For more information, see the *LogLogic Lasso Collector Users Guide*.

Figure 18 McAfee ePO with LogLogic Appliance Components and Processes



Once the data is captured and parsed, you can generate reports. In addition, you can create alerts to notify you of issues on McAfee ePO. For more information on creating reports and alerts, see the *LogLogic User Guide* and *LogLogic Online Help*.

Table 1 on page 38 lists the McAfee ePO events that are supported by the LogLogic Appliance.

> **Note:** The LogLogic Appliance only parses Event Logs. However, all other VSE log and ePO server log (i.e., Audit Log, Server Task Log, etc.) event information is available via reports and searching.

For more information, see *Appendix A – Event Reference* on page 37 for sample log messages for each event and event to category mapping.

LogLogic Real-Time Reports

LogLogic provides pre-configured Real-Time Reports for McAfee ePO log data.

The following Real-Time Reports are available:

- **All Unparsed Events**—Displays data for all events retrieved from the McAfee ePO log for a specified time interval
- **Configuration Report**—Displays information on the following data:
  - Client policy update status
  - Client upgrade status
  - Threat Management signature status
  - Threat Management engine status

- **HIPS Activity**— Displays information on the following data:
  - Intrusion detection
- **Scan Report**—Displays information on the following data:
  - Scan operations
  - Scan exclusions
  - Scan errors
- **Threat Report**—Displays information on the following data:
  - Malicious code
  - Quarantines
  - Buffer overflows
  - Intrusion detection
  - Infections
  - Access protection

To access LMI 5 Real-Time Reports:

1. In the top navigation pane, click **Reports**.
2. Select **Threat Management**.

   The following Real-Time Reports are available:
   - **Configuration Activity**
   - **HIPS Activity**
   - **Scan Activity**
   - **Threat Activity**
3. Select **Operational**.

   The following Real-Time Reports is available:
   - All Unparsed Events

You can create Custom Reports from the existing Real-Time Report templates. For more information, see the *LogLogic User Guide* and *LogLogic Online Help*.

LogLogic Search Filters

LogLogic provides pre-configured Search Filters for McAfee ePO log data. Search Filters are used to filter report data and create alerts.

To access Search Filters:

1. From the navigation menu, select **Search**.
2. Select **Search Filters**.

   The following Search Filters are available:

   - **McAfee VirusScan: A maximum load condition is occurring!**—Uses the following RegEx: `ThreatEventID="1512"`
   - **McAfee VirusScan: Activity log error**—Uses the following RegEx: `ThreatEventID="1040"`
   - **McAfee VirusScan: Activity log file maximum size reached**—Uses the following RegEx: `ThreatEventID="3033"`
   - **McAfee VirusScan: Agent: Cannot install software due to OS ver**—Uses the following RegEx: `ThreatEventID="2216"`
   - **McAfee VirusScan: Agent: Enforce task failed**—Uses the following RegEx: `ThreatEventID="2328"`
   - **McAfee VirusScan: Agent: Failed to install software package**—Uses the following RegEx: `ThreatEventID="2201"`
   - **McAfee VirusScan: Agent: Install retry limit reached**—Uses the following RegEx: `ThreatEventID="2202"`
   - **McAfee VirusScan: Agent: Insufficient disk space to download**—Uses the following RegEx: `ThreatEventID="2208"`
   - **McAfee VirusScan: Agent: Insufficient disk space to install**—Uses the following RegEx: `ThreatEventID="2204"`
   - **McAfee VirusScan: Agent: Property collection failed**—Uses the following RegEx: `ThreatEventID="2264"`
   - **McAfee VirusScan: Computers are non-compliant**—Uses the following RegEx: `ThreatEventID="16000"`
   - **McAfee VirusScan: Deployment failed**—Uses the following RegEx: `ThreatEventID="2412"`
   - **McAfee VirusScan: Deployment successful**—Uses the following RegEx: `ThreatEventID="2411"`
   - **McAfee VirusScan: Directory length access error**—Uses the following RegEx: `ThreatEventID="3008"`
   - **McAfee VirusScan: Disk I/O errors**—Uses the following RegEx: `ThreatEventID="(?:1047|3013)"`
   - **McAfee VirusScan: Encrypted/Corrupted item found**—Uses the following RegEx: `ThreatEventID="8501"`
   - **McAfee VirusScan: Error during initialization of the activity log file**—Uses the following RegEx: `ThreatEventID="3036"`
   - **McAfee VirusScan: Error launching a program upon virus infection**—Uses the following RegEx: `ThreatEventID="3035"`

- **McAfee VirusScan: Error obtaining device driver versions**—Uses the following RegEx: `ThreatEventID="3019"`
- **McAfee VirusScan: Error obtaining log data from device driver**—Uses the following RegEx: `ThreatEventID="3028"`
- **McAfee VirusScan: Error occurred starting log subsystem**—Uses the following RegEx: `ThreatEventID="3018"`
- **McAfee VirusScan: Error occurred while disabling driver**—Uses the following RegEx: `ThreatEventID="3030"`
- **McAfee VirusScan: Error occurred while enabling driver**—Uses the following RegEx: `ThreatEventID="3029"`
- **McAfee VirusScan: Error opening Service Manager**—Uses the following RegEx: `ThreatEventID="3016"`
- **McAfee VirusScan: Error sending alert**—Uses the following RegEx: `ThreatEventID="1062"`
- **McAfee VirusScan: Error sending exclude information to the driver**—Uses the following RegEx: `ThreatEventID="3026"`
- **McAfee VirusScan: Error sending move to folder to the driver**—Uses the following RegEx: `ThreatEventID="3027"`
- **McAfee VirusScan: Error sending new options to device driver**—Uses the following RegEx: `ThreatEventID="3025"`
- **McAfee VirusScan: Error starting drivers**—Uses the following RegEx: `ThreatEventID="3017"`
- **McAfee VirusScan: Error starting Task**—Uses the following RegEx: `ThreatEventID="1003"`
- **McAfee VirusScan: Error stopping drivers**—Uses the following RegEx: `ThreatEventID="3055"`
- **McAfee VirusScan: Error stopping scheduled task**—Uses the following RegEx: `ThreatEventID="1069"`
- **McAfee VirusScan: Error while obtaining statistical data from driver**—Uses the following RegEx: `ThreatEventID="3031"`
- **McAfee VirusScan: Error while stopping task**—Uses the following RegEx: `ThreatEventID="1005"`
- **McAfee VirusScan: Error while trying to open/create activity log file**—Uses the following RegEx: `ThreatEventID="3032"`
- **McAfee VirusScan: Error writing to log**—Uses the following RegEx: `ThreatEventID="3038"`
- **McAfee VirusScan: Failed quarantine check**—Uses the following RegEx: `ThreatEventID="18003"`
- **McAfee VirusScan: Failed to connect to CMA scheduler** (i.e., Common Management Agent)—Uses the following RegEx: `ThreatEventID="4701"`
- **McAfee VirusScan: Failed to connect to CMA updater**—Uses the following RegEx: `ThreatEventID="4700"`
- **McAfee VirusScan: Failed to save schedule data into CMA**—Uses the following RegEx: `ThreatEventID="4702"`
- **McAfee VirusScan: File I/O errors**—Uses the following RegEx: `ThreatEventID="(?:1046|3012)"`

- **McAfee VirusScan: Inbound email suspend for low disk**—Uses the following RegEx: `ThreatEventID="1507"`
- **McAfee VirusScan: Inbound email resumed**—Uses the following RegEx: `ThreatEventID="1508"`
- **McAfee VirusScan: Invalid options specified**—Uses the following RegEx: `ThreatEventID="1063"`
- **McAfee VirusScan: Item matched filtering criteria**—Uses the following RegEx: `ThreatEventID="8502"`
- **McAfee VirusScan: Item matched spam criteria**—Uses the following RegEx: `ThreatEventID="8503"`
- **McAfee VirusScan: Media is write protected**—Uses the following RegEx: `ThreatEventID="3009"`
- **McAfee VirusScan: Memory allocation error**—Uses the following RegEx: `ThreatEventID="(?:1077|3023)"`
- **McAfee VirusScan: Memory grant unavailable**—Uses the following RegEx: `ThreatEventID="3037"`
- **McAfee VirusScan: On-demand scan started**—Uses the following RegEx: `ThreatEventID="1202"`
- **McAfee VirusScan: Outbreak rule name**—Uses the following RegEx: `ThreatEventID="2100"`
- **McAfee VirusScan: Process ended**—Uses the following RegEx: `ThreatEventID="1201"`
- **McAfee VirusScan: Process started**—Uses the following RegEx: `ThreatEventID="1200"`
- **McAfee VirusScan: Report OS & Serial**—Uses the following RegEx: `ThreatEventID="1204"`
- **McAfee VirusScan: Rogue System Sensor started successfully**—Uses the following RegEx: `ThreatEventID="12000"`
- **McAfee VirusScan: Rogue System Sensor failed to start**—Uses the following RegEx: `ThreatEventID="12001"`
- **McAfee VirusScan: Rogue System Sensor stopped**—Uses the following RegEx: `ThreatEventID="12002"`
- **McAfee VirusScan: Scan settings**—Uses the following RegEx: `ThreatEventID="1089"`
- **McAfee VirusScan: Scan shut down by Windows**—Uses the following RegEx: `ThreatEventID="1129"`
- **McAfee VirusScan: Scan was canceled by autoupdate of DAT files**—Uses the following RegEx: `ThreatEventID="1126"`
- **McAfee VirusScan: Scheduled task was stopped**—Uses the following RegEx: `ThreatEventID="1068"`
- **McAfee VirusScan: Shutdown request successfully processed**—Uses the following RegEx: `ThreatEventID="1510"`
- **McAfee VirusScan: Spam email scanning statistics**—Uses the following RegEx: `ThreatEventID="4651"`
- **McAfee VirusScan: Specified media not found**—Uses the following RegEx: `ThreatEventID="3010"`

- **McAfee VirusScan: Specified scan item is invalid**—Uses the following RegEx: `ThreatEventID="3011"`
- **McAfee VirusScan: Startup request successfully processed**—Uses the following RegEx: `ThreatEventID="1509"`
- **McAfee VirusScan: Subnet has become unmonitored by Rogue System Sensor**—Uses the following RegEx: `ThreatEventID="16007"`
- **McAfee VirusScan: System Compliance Profiler rule violation**—Uses the following RegEx: `ThreatEventID="13002"`
- **McAfee VirusScan: Task error while accessing activity log file**—Uses the following RegEx: `ThreatEventID="3006"`
- **McAfee VirusScan: Task has completed successfully**—Uses the following RegEx: `ThreatEventID="1004"`
- **McAfee VirusScan: Task reported an internal application error**—Uses the following RegEx: `ThreatEventID="3015"`
- **McAfee VirusScan: Task reports general system error**—Uses the following RegEx: `ThreatEventID="3014"`
- **McAfee VirusScan: Task reports memory allocation error**—Uses the following RegEx: `ThreatEventID="3007"`
- **McAfee VirusScan: Task started ok**—Uses the following RegEx: `ThreatEventID="1066"`
- **McAfee VirusScan: Task started successfully**—Uses the following RegEx: `ThreatEventID="1002"`
- **McAfee VirusScan: Task was canceled**—Uses the following RegEx: `ThreatEventID="1071"`
- **McAfee VirusScan: Task was canceled**—Uses the following RegEx: `ThreatEventID="3001"`
- **McAfee VirusScan: Task was successful**—Uses the following RegEx: `ThreatEventID="1070"`
- **McAfee VirusScan: The machine is compliant or non-compliant with rules**—Uses the following RegEx: `ThreatEventID="13001"`
- **McAfee VirusScan: The update is running**—Uses the following RegEx: `ThreatEventID="1120"`
- **McAfee VirusScan: The upgrade is running**—Uses the following RegEx: `ThreatEventID="1122"`
- **McAfee VirusScan: Unable to start scheduled task**—Uses the following RegEx: `ThreatEventID="1067"`
- **McAfee VirusScan: Unable to write the activity log file**—Uses the following RegEx: `ThreatEventID="3034"`
- **McAfee VirusScan: Warning - abnormal termination!**—Uses the following RegEx: `ThreatEventID="1511"`

Note: All ePO Search Filters use Regular Expressions (RegEx) that can be used to create reports using **RegEx Search** features on the LogLogic Appliance.

For more information on Search Filters, reports, and alerts see the *LogLogic User Guide* and *LogLogic Online Help*.

Chapter 3 – Troubleshooting

This chapter contains troubleshooting information regarding the configuration and/or use of log collection for McAfee ePO. It also contains Frequently Asked Questions (FAQ), providing quick answers to common questions.

- Troubleshooting 35
- Frequently Asked Questions 36

Troubleshooting

Is your version of McAfee ePO supported?

For more information, see *Prerequisites* on page 7.

Is your LogLogic Appliance running Release 4.9.1 or later?

If you are running an release prior to 4.9.1, you will require an upgrade. Contact LogLogic Support for more information.

Is the appropriate Log Source Package (LSP) installed properly?

Check to make sure that the LSP that is installed includes support for McAfee ePO. Also make sure that the package was installed successfully. For more information on LSP installation procedures, see the *LogLogic Release Notes*.

If McAfee ePO log events are not appearing on the LogLogic Appliance...

You need to verify if the database connection information provided to the LogLogic Appliance is correct and that the connection is up and running. For more information, see *Adding a McAfee ePO Device* on page 23 and *Testing Connectivity* on page 26.

Did you receive the following error message: `Error Message: Refused connection: Login failed for user 'xyz'`?

Make sure that your ePO database is using Mixed Mode Authentication or SQL Authentication mode. Make sure that you have typed your SQL User account password correctly. Make sure that you can log in to the ePO database both remotely and locally using the Microsoft Query Analyzer tool using the same SQL User account. Logging into the ePO database in this way will test connectivity and verify if the SQL User account is correct.

Did you receive the following error message: `Error Message: Refused connection: The TCP/IP connection to the host has failed. java.net.ConnectException: Connection refused`?

Make sure that you have the correct port configured for the ePO server database instance and check to make sure that the port is open to the ePO server database by using telnet to access the port. Make sure that database name is correct. Make sure that you can log in to the ePO database remotely using the Microsoft Query Analyzer tool using the same SQL User account. Logging into the ePO database in this way will test connectivity and verify if the SQL User account is correct.

Frequently Asked Questions

How does the LogLogic Appliance collect logs from McAfee ePO?

LogLogic's Database Collector connects to the Microsoft SQL Server database on the ePO server via JDBC to capture the log data. For more information, see *How LogLogic Captures McAfee ePO Log Data* on page 28.

What access permissions are required?

To configure logging on McAfee ePO, the user must have the proper permissions to access the ePO Admin Console to make configuration changes. You also need to have a Microsoft SQL Server User account with `db_datareader` and `public` database role access at the minimum. For more information, see *Prerequisites* on page 7.

How do I configure logging on McAfee ePO?

Follow the procedures on *Configuring McAfee ePO* on page 8. Also make sure that you have properly added the device and configured the database server information on the LogLogic Appliance. For more information, see *Adding a McAfee ePO Device* on page 23.

How do I locate the ePO server port number?

1. On database server for ePO, launch the **Server Network Utility** located under Windows **Start menu > Programs > Microsoft SQL Server**.
2. On the **General** tab, select the ePO server database instance from the drop-down menu.
3. From the **Enable Protocols** list, select **TCP/IP**, then select **Properties**.

Appendix A – Event Reference

This appendix lists the LogLogic-supported McAfee ePO events. The McAfee ePO event table identifies events that can be analyzed through LogLogic reports. All sample log messages were captured by the LogLogic's Database Collector on the LogLogic Appliance.

LogLogic Support for McAfee ePO Events

The following list describes the contents of each of the columns in the tables below.

- **Event ID** – McAfee ePO event identifier
- **Agile Reports/Search** – Defines if the McAfee ePO event is available through the LogLogic Agile Report Engine or through the search capabilities. If the event is available through the Agile Report Engine, then you can use LogLogic's Real-Time Reports and Summary Reports to analyze and display the captured log data. Otherwise, all other supported events that are captured by the LogLogic Appliance can be viewed by performing a search for the log data.
- **Title/Comments** – Description of the event
- **Event Category** – Category of events such as Normal operation, Software failure or error, etc.
- **Event Type** – Type of event such as Success, Failure, etc.
- **Reports Appears In** – LogLogic-provided reports that the event appears in
- **Sample Log Message** – Sample McAfee ePO log messages

Table 1 McAfee ePO Events

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
1	1024	Agile	Infected file found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
2	1025	Agile	Infected file successfully Cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
3	1026	Agile	Unable to clean infected file	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
4	1027	Agile	Infected file deleted	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
5	1028	Agile	Unable to delete infected file	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
6	1029	Agile	File to be excluded from scans	Normal operation	Success	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
7	1030	Agile	Unable to exclude item from scans	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
8	1031	Agile	Infected file access denied	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
9	1032	Agile	Infected file was moved to quarantine area	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
10	1033	Agile	Unable to move infected file to quarantine	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
11	1034	Agile	Scan completed. No viruses found	Normal operation	Success	Configuration Report	108 D4370307-5A54-45B2-9458-B5A12E99A582 2003-1 53:19.5 53:06.0 6B4427F5-A9E9-4B14-BFA7-60DBE3B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100082 5233 5200.216 Full Scan XPPRO-1 739246210 0x00000000000000000000FFFFAC100082 cotto ops.task.end 1034 6 1 Normal operation Scan completed. No viruses found.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
12	1035	Agile	Scan was cancelled	Scan cancelled	Cancel	Scan Report	142 0BA12BA5-7AFC-4E33-938A-35CD D15CCF79 2003-1 19:07.6 18:52.0 6B4427F5-A9E9-4B14-BFA7-60DBE3 B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 5233 5200.216 OAS XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 XPPRO-1\cotto C:\Documents and Settings\cotto\Local Settings\Temporary Internet Files\Content.IE5\Q777CJN6\goog le[1]\google[1] av 1051 1 0 Software failure or error Unable to scan password protected
13	1036	Agile	Memory infected	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
14	1037	Agile	Infected boot record found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
15	1038	Agile	Scan found infected files	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
16	1039	Agile	Scan found and cleaned infected files	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
17	1041	Agile	Scan reports memory allocation error	Software failure or error	Error	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
18	1042	Agile	Path too long	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
19	1043	Agile	Media is write protected	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
20	1044	Agile	Specified media not found	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
21	1045	Agile	Specified scan item is invalid	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
22	1048	Agile	Scan reports general system error	Software failure or error	Error	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
23	1049	Agile	Scan reported an internal application error	Software failure or error	Error	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
24	1050	Agile	Unable to repair password protected	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
25	1051	Agile	Unable to scan password protected	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
26	1052	Agile	Infected Binder Object	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
27	1053	Agile	Infected file found	Virus detected (heuristic) and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
28	1054	Agile	Infected file deleted	Virus detected (heuristic) and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
29	1055	Agile	Unable to delete infected file	Virus detected (heuristic) and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
30	1056	Agile	File moved to quarantine	Virus detected (heuristic) and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
31	1057	Agile	Unable to move infected file to quarantine	Virus detected (heuristic) and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
32	1059	Agile	Scan Timed Out	Software failure or error	Failure	Scan Report	241 02D9BE90-B80B-4195-A762-010A9D D54AA4 2003-1 11:32.1 04:28.0 6B4427F5-A9E9-4B14-BFA7-60DBE3 B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 5234 5200.216 OAS XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 NT AUTHORITY\SYSTEM C:\Program Files\Common Files\McAfee\Engine\avvscan.dat av 1059 1 virus 0 Software failure or error Scan Timed Out
33	1060	Agile	Boot sector virus was cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
34	1061	Agile	Error while cleaning boot sector virus	Virus detected and NOT removed	Error	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
35	1064	Agile	Service was started	Normal operation	Success	Configuration Report	254 35FFAC38-AFAB-4DAB-8097-08E15 18B8D63 2003-1 13:35.5 30:17.0 26651266-2598-4891-9A6E-319CF785 1065 VIRUSCAN8600 VirusScan Enterprise 8.5 2003-1 739246267 0x00000000000000000000FFFFAC100 0BB 4.0.0 0.0.0 OAS 2003-1 739246267 0x00000000000000000000FFFFAC100 0BB SYSTEM ops.service.start 1064 6 1 Normal operation Service was started.
36	1065	Agile	Service ended	Normal operation	Success	Configuration Report	270 D81D856E-DD7B-42A5-A7D2-12416 A764352 2003-1 29:37.9 21:40.0 26651266-2598-4891-9A6E-319CF785 1065 VIRUSCAN8600 VirusScan Enterprise 8.5 2003-1 739246267 0x00000000000000000000FFFFAC100 0BB 5233 5200.216 OAS 2003-1 739246267 0x00000000000000000000FFFFAC100 0BB 172.16.0.187 ops.service.end 1065 6 1 Normal operation Service ended.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
37	1076	Agile	Error logging information	Software failure or error	Error	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
38	1086	Agile	Scan Process Error	Software failure or error	Error	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
39	1087	Agile	On-access Scan started	Normal operation	Success	Scan Report	272 40B288DC-B2A8-4DA8-BCFF-AF234313410B 2003-1 29:38.0 24:29.0 26651266-2598-4891-9A6E-319CF7851065 VIRUSCAN8600 VirusScan Enterprise 8.5 2003-1 739246267 0x00000000000000000000FFFFAC1000BB 4.0.0 0.0.0 OAS 2003-1 739246267 0x00000000000000000000FFFFAC1000BB SYSTEM ops.scan.start 1087 6 1 Normal operation On-access Scan started
40	1088	Agile	On-access scan stopped	Normal operation	Success	Scan Report	273 54B2A14D-9FA3-411F-B6D6-F530D7738763 2003-1 29:38.0 29:33.0 26651266-2598-4891-9A6E-319CF7851065 VIRUSCAN8600 VirusScan Enterprise 8.5 2003-1 739246267 0x00000000000000000000FFFFAC1000BB 5233 5200.216 OAS 2003-1 739246267 0x00000000000000000000FFFFAC1000BB SYSTEM ops.scan.end 1088 6 1 Normal operation On-access scan stopped.
41	1090	Agile	OAS stopped	On-access scan disabled	Pause	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
42	1091	Agile	JavaScript security violation detected and blocked	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
43	1092	Agile	Access Protection rule violation detected and blocked	Access Protection rule violation detected and blocked	Success	Threat Report	949 AD650930-6BC1-4358-B313-DAEF4 D6E8BEB 2003-1 14:11.1 01:12.0 6B4427F5-A9E9-4B14-BFA7-60DBE3 B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 OAS XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 XPPRO-1\cotto C:\WINDOWS\Explorer.EXE C:\Documents and Settings\cotto\Local Settings\Temp\IXP000.TMP\Install .exe hip.file 1092 5 Common Standard Protection:Prevent common programs from running files from the Temp folder access protection deny execute 1 Access Protection rule violation detected and blocked Access Protection rule violation detected and blocked
44	1093	Agile	Buffer Overflow detected and blocked	Buffer Overflow detected and blocked	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
45	1094	Agile	Port blocking rule violation detected	Access Protection rule violation detected and blocked (threat)	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
46	1095	Agile	Access Protection rule violation detected and NOT blocked	Access Protection rule violation detected and NOT blocked	ALLOWED	Threat Report	975 59C36CDB-7178-4BA7-B6F7-C341FE0A53EE 2003-1 15:45.9 12:24.0 6B4427F5-A9E9-4B14-BFA7-60DBE3B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 -16777215 0x00000000000000000000FFFF7F000001 OAS XPPRO-1 -16777215 0x00000000000000000000FFFF7F000001 XPPRO-1\cotto C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\mscorsvw.exe C:\WINDOWS\assembly\NativeImages_v2.0.50727_32\Temp\ZAP59.tmp\mscorlib.dll hip.file 1095 5 Common Maximum Protection:Prevent creation of new executable files in the Windows folder access protection would deny create 1 Access Protection rule violation detected and NOT blocked Access Protection rule violation detected and NOT blocked
47	1099	Agile	Buffer Overflow detected and NOT blocked	Buffer Overflow detected and NOT blocked	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
48	1100	Agile	Macro Detected in file	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
49	1101	Agile	Macro Deleted from file	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
50	1118	Agile	The update was successful	Update/ upgrade succeeded	Success	Configuration Report	1118 7C9A9D6C-567D-44F9-A8E3-4C6B6F48D794 2003-1 59:56.4 58:34.0 26651266-2598-4891-9A6E-319CF7851065 VIRUSCAN8600 VirusScan Enterprise 8.5 2003-1 739246267 0x00000000000000000000FFFFAC1000BB 5233 5200.216 AutoUpdate 2003-1 739246267 0x00000000000000000000FFFFAC1000BB SYSTEM ops.update.end 1118 6 1 Update/upgrade succeeded The update was successful
51	1119	Agile	The update failed; see event log	Update/ upgrade failed	Failure	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
52	1121	Agile	The update was cancelled	Update/ upgrade failed	Cancel	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
53	1123	Agile	The upgrade failed; see event log	Update/ upgrade failed	Failure	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
54	1124	Agile	The upgrade was cancelled	Update/ upgrade failed	Cancel	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
55	1125	Agile	The DAT version was not new enough	Update/ upgrade failed	Failure	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
56	1127	Agile	OAS Scanning Engine Disabled	On-access scan disabled	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
57	1128	Agile	Scan time exceeded	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
58	1203	Agile	On Demand scan complete	Normal operation	Success	Scan Report	109 B8CC6DA6-6D95-476F-95D5-CE67F064DB0F 2003-1 53:39.4 53:06.0 6B4427F5-A9E9-4B14-BFA7-60DBE3B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100082 5233 5200.216 Full Scan XPPRO-1 739246210 0x00000000000000000000FFFFAC100082 cotto ops.task.end 1203 6 1 Normal operation On Demand scan complete
59	1270	Agile	File infected. No cleaner available, quarantined successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
60	1271	Agile	File infected. No cleaner available, heuristic detection, quarantined successfully	Virus detected (heuristic) and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
61	1272	Agile	File infected. Undetermined clean error, quarantined successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
62	1273	Agile	File infected. Clean error, Encrypted file, quarantined successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
63	1274	Agile	File infected. No cleaner available, quarantine failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
64	1275	Agile	File infected. No cleaner available, heuristic detection, quarantine failed	Virus detected (heuristic) and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
65	1276	Agile	File infected. Undetermined clean error, quarantine failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
66	1277	Agile	File infected. Clean error, Encrypted file, quarantine failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
67	1278	Agile	File infected. No cleaner available, file deleted successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
68	1279	Agile	File infected. No cleaner available, heuristic detection, deleted successfully	Virus detected (heuristic) and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
69	1280	Agile	File infected. Undetermined clean error, deleted successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
70	1281	Agile	File infected. Clean error, Encrypted file, deleted successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
71	1282	Agile	File infected. No cleaner available, delete failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
72	1283	Agile	File infected. Clean error, heuristic detection, delete failed	Virus detected (heuristic) and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
73	1284	Agile	File infected. Undetermined clean error, delete failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
74	1285	Agile	File infected. Clean error, Encrypted file, delete failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
75	1286	Agile	File infected. No cleaner available, continued scanning (ODS)	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
76	1287	Agile	File infected. Clean error, heuristic detection, continued scanning (ODS)	Virus detected (heuristic) and NOT removed	Error	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
77	1288	Agile	File infected. Undetermined clean error, continued scanning (ODS)	Virus detected and NOT removed	Error	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
78	1289	Agile	File infected. Clean error, Encrypted file, continued scanning (ODS)	Virus detected and NOT removed	Error	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
79	1290	Agile	File infected. No cleaner available, OAS denied access and continued	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
80	1291	Agile	File infected. Clean error, heuristic detection, OAS denied access and continued	Virus detected (heuristic) and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
81	1292	Agile	File infected. Undetermined clean error, OAS denied access and continued	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
82	1293	Agile	File infected. Quarantine failed, deleted successfully	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
83	1294	Agile	File infected. Quarantine failed, deleted failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
84	1295	Agile	File infected. Move failed, continued scanning (ODS)	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
85	1296	Agile	File infected. Move failed, denied access and continued (OAS)	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
86	1297	Agile	File infected. Delete failed, quarantined	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
87	1298	Agile	File infected. Delete failed, quarantine failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
88	1299	Agile	File infected. Delete failed, continued scanning (ODS)	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
89	1300	Agile	File infected. Delete failed, denied access and continued (OAS)	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
90	1500	Agile	Infected email cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
91	1501	Agile	Infected email quarantined	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
92	1502	Agile	Unable to clean infected mail	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
93	1503	Agile	Infected email detected	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
94	1504	Agile	Infected mail item deleted	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
95	1505	Agile	Email content filtered	E-mail content filtered or blocked	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
96	1506	Agile	Email content blocked	E-mail content filtered or blocked	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
97	1513	Agile	Mail virus quarantined and cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
98	1514	Agile	Mail virus quarantined (not cleaned)	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
99	2000	Agile	Infected file found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
100	2001	Agile	Infected file successfully cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
101	2002	Agile	Unable to clean infected file	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
102	2003	Agile	Infected file deleted	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
103	2004	Agile	Unable to delete infected file	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
104	2005	Agile	File to be excluded from scans	Normal operation	Success	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
105	2006	Agile	Unable to exclude item from scans	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
106	2007	Agile	Infected file access denied	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
107	2008	Agile	Infected file was moved to quarantine area	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
108	2009	Agile	Unable to move infected file to quarantine	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
109	2020	Agile	Boot record infection found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
110	2021	Agile	Boot record infection cleaned	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
111	2022	Agile	Boot record infection clean error	Virus detected and NOT removed	Error	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
112	2023	Agile	New File Virus Found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
113	2024	Agile	New File Virus Found And Deleted	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
114	2025	Agile	New File Virus Found But Move Failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
115	2026	Agile	New File Virus Found And Moved	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
116	2027	Agile	New File Virus Found But Move Failed	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
117	2028	Agile	MBR Virus Found	Virus detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
118	2401	Agile	Update Successful	Update/ upgrade succeeded	Success	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
119	2402	Agile	Update Failed	Update/ upgrade failed	Failure	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
120	2413	Agile	Attempt to uninstall McAfee Agent	Attempt to uninstall ePolicy Orchestrator Agent	DENIED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
121	3000	Agile	Scan task completed. No viruses found	Normal operation	Success	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
122	3002	Agile	Virus found in Memory	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
123	3003	Agile	Infected boot record found	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
124	3004	Agile	Task found infected files	Virus detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
125	3005	Agile	Task found and cleaned infected files	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
126	3012	Agile	File I/O errors	Software failure or error	Error	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
127	3020	Agile	Invalid virus signature files	Software failure or error	Failure	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
128	3021	Agile	Scan engine error	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
129	3022	Agile	Initialization error with scan buffer	Software failure or error	Failure	Scan Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
130	3024	Agile	Unknown error reported	Software failure or error	Error	Configuration Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
131	4650	Agile	Detected Spam Email	Spam detected and handled	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
132	8000	Agile	Infected item found	Virus detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
133	8500	Agile	Banned item found	Banned content or file detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
134	16006	Agile	New Rogue System detected	New Rogue System detected	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
135	18000	Agile	Host intrusion detected and handled	Host intrusion detected and handled	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
136	18001	Agile	Network intrusion detected and handled	Network intrusion detected and handled	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
137	18002	Agile	Application blocked	Application blocked	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
138	21024	Agile	Unwanted program found	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
139	21025	Agile	Unwanted program successfully cleaned	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
140	21026	Agile	Unable to clean unwanted program	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
141	21027	Agile	Unwanted program deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
142	21028	Agile	Unable to delete unwanted program	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
143	21031	Agile	Unwanted program access denied	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
144	21032	Agile	Unwanted program was moved to quarantine area	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
145	21033	Agile	Unable to move unwanted program to quarantine	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
146	21036	Agile	Unwanted program found in memory	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
147	21054	Agile	Unwanted program deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
148	21055	Agile	Unable to delete unwanted program	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
149	21056	Agile	Unwanted program moved to quarantine	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
150	21057	Agile	Unable to move unwanted program to quarantine	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
151	21270	Agile	Unwanted program quarantined-no cleaner	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
152	21271	Agile	Unwanted program quarantined, Heuristics	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
153	21272	Agile	Unwanted program quarantined, can't clean	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
154	21273	Agile	Unwanted program quarantined, encrypted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
155	21274	Agile	Unwanted program not cleaned or quarantined	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
156	21275	Agile	Unwanted program, heuristics, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
157	21276	Agile	Unwanted program, clean error, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
158	21277	Agile	Unwanted program, encrypted, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
159	21278	Agile	Unwanted program, no cleaner, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
160	21279	Agile	Unwanted program, heuristics, no cleaner, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
161	21280	Agile	Unwanted program, clean error, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
162	21281	Agile	Unwanted program, encrypted, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
163	21282	Agile	Unwanted program, no cleaner, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
164	21283	Agile	Unwanted program, heuristics, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
165	21284	Agile	unwanted program, clean error, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
166	21285	Agile	Unwanted program, encrypted, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
167	21286	Agile	Unwanted program, no cleaner, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
168	21287	Agile	Unwanted program, heuristics, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
169	21288	Agile	Unwanted program, clean error, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
170	21289	Agile	Unwanted program, encrypted, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
171	21290	Agile	Unwanted program, no cleaner, denied access	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
172	21291	Agile	Unwanted program, heuristics, denied access	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
173	21292	Agile	Unwanted program, clean error, denied access	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
174	21293	Agile	Unwanted program, quarantine failed, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
175	21294	Agile	Unwanted program, quarantine failed, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
176	21295	Agile	Unwanted program, quarantine failed, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
177	21296	Agile	Unwanted program, quarantine failed, denied access	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
178	21297	Agile	Unwanted program, delete failed, quarantined	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
179	21298	Agile	Unwanted program, delete failed, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
180	21299	Agile	Unwanted program, delete failed, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
181	21300	Agile	Unwanted program, delete failed, denied access	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
182	21400	Agile	User-specified unwanted program found	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
183	21401	Agile	User-specified unwanted program	Unwanted program detected and NOT removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
184	21402	Agile	User-specified unwanted program, clean error, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
185	21403	Agile	User-specified unwanted program, clean error, quarantined	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
186	21404	Agile	User-specified unwanted program, clean error, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
187	21405	Agile	User-specified unwanted program, clean error, deleted	Unwanted program detected and removed	Success	Threat Report	442 4DF2D589-A8A7-4FC2-A75A-E7A4 864901CB 2003-1 36:27.6 36:24.0 6B4427F5-A9E9-4B14-BFA7-60DBE3 B3287E VIRUSCAN8600 VirusScan Enterprise 8.5 XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 5234 5200.216 OAS XPPRO-1 739246210 0x00000000000000000000FFFFAC100 082 XPPRO-1\cotto C:\WINDOWS\system32\ftp.exe av.pup 21405 1 User defined detection: FTP app_pua deleted 1 Unwanted program detected and removed User-specified unwanted program, clean error, deleted
188	21406	Agile	User-specified unwanted program was moved to quarantine area	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
189	21407	Agile	User-specified unwanted program, quarantine failed, delete failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
190	21408	Agile	User-specified unwanted program, quarantine failed, deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
191	21409	Agile	User-specified unwanted program, quarantine failed, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
192	21410	Agile	User-specified unwanted program deleted	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.

#	Event ID	Agile Reports/ Search	Title/Comments	Event Category	Event Type	Reports Appears In	Sample Log Message
193	21411	Agile	User-specified unwanted program, delete failed, quarantine failed	Unwanted program detected and NOT removed	Failure	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
194	21412	Agile	User-specified unwanted program, delete failed, quarantine	Unwanted program detected and removed	Success	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.
195	21413	Agile	User-specified unwanted program, delete failed, continued	Unwanted program detected and NOT removed	ALLOWED	Threat Report	The log format for this event is supported by the LogLogic Appliance, but the event has not been fully validated by LogLogic. Therefore no sample log message is available. For more information on this event, see the McAfee Product Documentation.